OVERSIGHT BOARD - APPLICANT PRIVACY NOTICE

Last Updated: 12 March 2020

1. What is the purpose of this document?

Oversight Board LLC and Oversight Board UK Limited (together referred to as "we" or "Oversight Board") are committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal data information about you when you apply to work with us.

This privacy notice applies to all applicants worldwide. However, there are some aspects of this notice which only apply to specified jurisdictions, which we have set out below in this notice.

We may be required under applicable data protection legislation to notify you of the information contained in this privacy notice. We provide you with this notice in the interests of transparency and, to the extent that this applies, to satisfy any relevant obligation we might have under data protection legislation in relation to our handling of your personal information in connection with your application.

This notice does not form part of any contract of employment or other contract to provide services. The giving of this notice does not indicate any promise or offer of employment or other contract to provide services.

We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

2. Data protection principles

We will comply with applicable data protection law. The personal information we hold about you will be:

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

3. The kind of information we hold about you

Personal data or personal information means any information that identifies, relates to, describes, or is reasonably capable of being associated with or linked to an individual. It does not include de-identified or anonymous data.

In connection with your application for work with us, we may collect, store and use the following categories of personal information about you:

- Identifiers, such as your name (including any former names and your mother's maiden name), home address (including proof of residence such as utility bills), previous addresses (including dates of residence at each address), telephone numbers, personal email address(es), gender, city, country and date of birth, nationality and the name and contact information of your references.
- Government or national identification information, such as a copy of your passport, passport number, country of passport issue, visa documentation, national ID card type and number and work authorization information.
- Financial information, such as your salary requirements and compensation history, including the results of searches of the bankruptcy register, credit checks and court litigation searches.
- Characteristics of protected classifications, such as your gender or age, where this collection is permitted by law.
- Audio, electronic, visual or similar information, such as CCTV footage from security cameras in our offices if you interview in person.
- Professional or employment-related information, such as your employment history, evidence of employment (such as contracts, offer letters and payslips), employee performance data, professional memberships and qualifications, regulatory body registration and status, current and previous directorship appointments and any other information contained in your CV, cover letter, or provided by your references.
- Education information, such as the institutions you attended, education transcripts or degrees you received.
- Inferences or views from you or about you, such as notes made during the interview process or the results of background searches (if applicable).

For residents of the EEA and UK, please also consider the section below concerning "**Special categories of information**".

4. How we collect the information

We collect personal information about applicants through the application and recruitment process, either directly from applicants and/or sometimes from an employment or recruitment agency, background check providers, credit reference agencies, your named references, the Home Office and from publicly accessible sources (in particular Facebook, LinkedIn, Twitter and other social media).

5. How we will use information about you

We use the categories of personal information in the list above to support our recruitment and hiring process, including:

- Application evaluation, such as assessing your skills, qualifications and suitability for the work or role and deciding whether to enter into a contract with you.
- Operational purposes, such as retaining records relating to our hiring processes, carrying out background and reference checks, where applicable, and communicating with you about the recruitment and hiring process.
- Legal and compliance purposes, such as implementing internal policies, responding to suspected fraud or other illegal activity, protecting our or others' rights and property, and complying with laws, legal processes, or government requests.

If you do not provide information necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to successfully process your application. For example, if we require references for this role and you do not provide us with relevant details, we may not be able to advance your application.

6. How we may share the information

We may need to share your data with third parties for the purposes of processing your application, such as our professional advisers and search consultancies. In addition, we may share your personal information in the following limited circumstances:

- With our personnel and affiliates, including other entities in the group, to carry out human resources and other business operations, as well as external third parties that perform these operations on our behalf or at our request (such as background check companies);
- With legal or regulatory authorities to comply with our obligations, protect the rights and property of us, our employees, and other stakeholders, and to detect and respond to suspected illegal activity and threats to the safety of any person or of our systems or services;
- In connection with any restructuring of our organisation; and
- With your consent or at your direction.

We require third parties to respect the security of your data and to treat it in accordance with the law. We or any third party with whom your data is shared may transfer for personal information outside your home jurisdiction. If we or they do, you can expect a similar degree of protection in respect of your personal information.

All 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.

7. Data Security

We have put in place measures to protect the security of your information.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In

addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a need to know.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

8. Data retention

We keep your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. We will retain your personal information for a period of 6 months after we have communicated to you our decision about whether to appoint you to the role applied for, and for any further period that we may determine is required for the purposes for which we retain this data. We retain your personal information so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After these purposes are satisfied we will securely destroy your personal information in accordance with applicable laws and regulations.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period for these purposes.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

9. How to update your data

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 recruitment process.

10. Information for Residents of the European Economic Area and United Kingdom

This section in blue only applies to you if you a resident of the European Economic Area (EEA) or United Kingdom (UK), in which case, please read the information below, which provides information about the data controller for your personal information and your rights and protections under the law regarding the processing of your personal information.

Oversight Board UK Limited is a **data controller**. This means that we are responsible for deciding how we hold and use personal information about you.

This is our "appropriate policy document" setting out how we will protect special categories of personal data and criminal convictions data. This meets the requirement of the UK Data Protection Act 2018 that an appropriate policy document be in place where processing special categories of personal data and criminal convictions data in certain circumstances.

Special categories of information

In addition to the information identified in section 3 above, we may also collect, store and use the following **special categories** of more sensitive personal data which require a higher level of protection under applicable law:

- Information about your race or ethnicity, religious or philosophical beliefs, sexual orientation and political opinions
- Information about your health, including any medical condition, health and sickness records
- Genetic information and biometric data
- Information about criminal convictions, allegations, proceedings and offenses

Legal basis for processing

The situations in which we will use your personal data described in section 5 above correspond to the following legal bases for processing under applicable law:

- Where we need it to consider entering into a contract with you
- Where we need to comply with a legal obligation
- Where you give us your consent; and
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

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.

How we use particularly sensitive personal information

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.
- In relation to information about your disability status, where it is needed to assess whether we need to provide any appropriate adjustments during the recruitment process, for example, during an interview, subject to appropriate confidentiality safeguards.

- In relation to information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions allegations, proceedings and offences (together “criminal convictions”) where the law allows us to do so.

We envisage that we may collect and hold information about your criminal convictions history in order to assess your fitness for a role you have applied for (where relevant) and if we would like to offer you the role (conditional on checks and any other conditions, such as references, being satisfactory). We will only do so if it is appropriate given the nature of the role and where we are legally able to do so. We may approach you for your consent for this in some circumstances, and where we do, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Transferring information outside the EEA

We will transfer the personal information we collect about you to the United States of America and may also transfer your personal information to other countries within and outside the EEA in order to process your application or where we have another legitimate interest in doing so or where sharing this information is in the legitimate interests of another third party (where your interests and fundamental rights do not override those legitimate interests), or if any other circumstance under section 5 applies.

There is not an adequacy decision by the European Commission in respect of the United States of America and this may also be the case with other relevant countries. This means that these to which we may transfer your data are not deemed to provide an adequate level of protection for your personal information.

However, to ensure that your personal information does receive an adequate level of protection we have or will put in place the appropriate measure(s) to ensure that your personal information is treated by those third parties in a way that is consistent with and which respect the EEA and UK laws on data protection. If you require further information about this, you can request it by emailing dataprotection@osbadmin.com.

Rights of access, correction, erasure, and restriction

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact by emailing dataprotection@osbadmin.com.

Right to withdraw consent

Where we process your personal information on the basis of your consent, you have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact by emailing dataprotection@osbadmin.com. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our data protection policy, we will dispose of your personal data securely.

No fee usually required

You will not usually have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it. **How to complain**

If you have any questions about this privacy notice or how we handle your personal information, please contact by emailing dataprotection@osbadmin.com. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, at ico.org.uk/concerns/ or telephone: 0303 123 1113.

11. Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information, where applicable.

If you have any questions about this privacy notice, please contact us at dataprotection@osdadmin.com.