NOMURA RESEARCH INSTITUTE EUROPE LIMITED
WEBSITE PRIVACY POLICY

Nomura Research Institute Europe Limited respects the privacy and rights of all individuals and takes very seriously its responsibilities under the data protection and privacy laws which apply to our business.

This privacy policy explains how and why we use personal data, and what we do to ensure that your information is kept safe and secure in accordance with the General Data Protection Regulation and any other applicable data protection and privacy laws including the UK Data Protection Act 2018 (**Data Protection Laws**).

This policy explains:

1. WHO WE ARE AND HOW TO CONTACT US

We are Nomura Research Institute Europe Limited (**NRIE**), a limited liability company with registered number 02175366, having our registered office and main place of business at 1 Angel Lane, London, England, EC4R 3AB.

NRIE also has a branch in Luxembourg (**NRIE Luxembourg**), details of which are available on our website (https://www.nri.com/global/company/office/europe/nri_europe.html).

References herein to the **Company**, **we**, **our**, or **us** refer, as appropriate, to NRIE or to NRIE Luxembourg depending on whether your personal data is being processed by NRIE or by NRIE Luxembourg.

NRIE's President has been appointed as our Head of Data Protection Compliance with overall responsibility for the data processing activities of NRIE and NRIE Luxembourg. If you have a query about how we process your personal data or wish to exercise your rights as a data subject then please contact us by:

- Emailing us at: nri-europe-cont@nri.co.jp
- Writing to us at our office address above, for the attention of President and Head of Data Protection Compliance;
- Telephoning us on +44(0)20-7521-1600.

For the purposes of Data Protection Laws, we are a controller in relation to much of the personal data we collect and process. This means that we are responsible

for deciding how and why we use personal data, and for keeping it safe. NRIE is registered as a data controller with the Information Commissioner's Office (**ICO**) with registration number *ZA377688*.

2. HOW WE COLLECT AND PROCESS PERSONAL DATA

A. BUSINESS, PROFESSIONAL AND OTHER CONTACTS

How we collect personal data

We collect and process personal data (meaning information which relates to an identified or identifiable individual) relating to individual business and professional contacts and other people we engage with in the course of our business, such as the employees of our corporate customers. Usually this information is:

- provided by the individuals themselves;
- collected in the process of providing consulting and business services to our corporate customers (such as through email correspondence and exchanging business cards);
- provided to us by third parties (such as other businesses we work with); or
- obtained from external sources (such as Companies House information on company directors).

The types of personal data we collect

The types of personal data we hold about these individuals typically consists of some or all of the following:

- contact information (such as name, address, telephone and email address);
- bank details (provided by a supplier and processed when we receive or make a payment).

There may of course be situations where we may process other types of personal data in the course of providing consulting and business services to our corporate customers, receiving goods and services from our suppliers and promoting our business. If we do, then it will be protected to the same high standards explained in this policy.

Why we need to use personal data

Depending on the circumstances, and the nature of our relationship with the people involved, we may use your personal data to:

- fulfil our contractual obligations or exercise contractual rights (such as paying our suppliers);
- communicate with other organisations, advisers or intermediaries; or
- send business related communications (usually by email);
- comply with our legal obligations;
- pursue our legitimate interests in operating and promoting the success of our business, or to pursue the interests of our corporate customers in providing our consulting and business services.

If we need to use your personal data for a purpose which is different to the purpose for which we originally collected it then we will notify you and explain the legal basis which allows us to do so.

B. RECRUITMENT

We collect, store and use personal data about individuals who apply to join us. This may include information:

- you provide to us (such as in CVs, application forms, and through correspondence);
- you provide during an interview;
- obtained from previous employers and referees;
- provided to us by recruitment agencies; and
- received as a result of our carrying out background checks (such as checks for criminal convictions with the Disclosure and Barring Service).

The information we collect might include sensitive personal data, such as information about your health and sickness records. If we need to process sensitive personal data then we will ask for your explicit consent before doing so.

If you apply for a position with us, we may carry out a check for criminal convictions in order to satisfy ourselves that there is nothing in your history which makes you unsuitable for the role. We do this because working with us involves a high degree of trust (as you will have access to confidential information).

We only carry out criminal records checks and ask for references at the last stage of the application process, when making an offer of employment, and always act in accordance with the specific requirements of Data Protection Laws and other applicable national laws.

How we use applicant information

We use the personal data we collect about you to:

- assess your skills, qualifications, and suitability for a role;
- carry out background and reference checks;
- communicate with you about your application;
- keep records related to our hiring process; and
- comply with legal or regulatory requirements.

We do all of this because either it is a necessary part of entering into a contract of employment with you or because we have a legitimate interest in ensuring that you are suitable for a particular role.

If you fail to provide personal data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully.

If we need to process sensitive personal data about a job applicant, for example disability information in order to consider whether we need to provide appropriate adjustments during the recruitment process, we will ask for explicit consent to do this at the time at which we request the data.

Retention of applicant information

We normally retain personal data about unsuccessful candidates for between 3 and 6 months from the time we inform them of our hiring decision. We retain personal data for this period so that we can demonstrate, in the event of a legal claim, we have not discriminated against an applicant and that the recruitment process was fair and transparent. After this period, we will securely destroy an applicant's personal data. If we wish to retain personal data on file, in case future opportunities arise, we will contact the applicant and ask for his or her consent to do so.

If you are successful, the personal data you provided in the application process will be stored as part of your personnel file.

3. COOKIES AND WEBSITE VISITORS

We do not normally collect personal data about visitors to our website unless they choose to provide such information when they contact us.

We collect anonymous information about visitors to our website in order to optimise and improve the website. This might include IP addresses, browser or device details and the connection type (for example, the Internet service provider used). However, none of this information will by itself directly identify any particular user.

Cookies

We use cookies to collect limited information about users of our websites, for diagnostic and analytic purposes.

If you do not want us to use cookies in your browser, you can remove cookies from your computer's hard drive, or set your browser to block cookies or to send a warning notice before a cookie is stored on your computer. However, please note that you may not be able to use many of the services on our website or other websites without cookies.

More detailed information on cookies can be found at www.allaboutcookies.org

Hyperlinks to other sites

Our website may include links to third-party websites or to other software applications or plug-ins. We are not responsible for the content or functionality of any of those external websites. If an external website requests personal data from you, the information you provide will not be covered by this policy. We suggest you read the privacy policy of any website before providing any personal data.

4. RECIPIENTS OF PERSONAL DATA

Personal data you provide to us will be kept private and confidential and except as set out in this policy we will not disclose or share it with other data controllers without your permission. The only exception to this is where we are legally required to disclose personal data. For example, to comply with a court order. We may also be required to share personal data with regulatory authorities (including the Information Commissioner's Office) in the event of an audit or investigation.

We share personal data with some of the third parties who provide services to our firm. This includes software and cloud service providers and IT support services. However, these third parties will only process personal data (which may include your information) on our behalf for specified purposes and in accordance with our strict instructions.

We only use third party service providers who have provided sufficient guarantees, as required by Data Protection Laws, that your personal data will be kept safe. We always ensure there is a written contract in place which protects your personal data and prevents it from being used for any purpose other than providing services to our business, in accordance with Data Protection Laws.

We may also share your personal data within the NRI group of companies where this is necessary for the purposes for which it was obtained and in accordance with the safeguards explained in section 7 (International Transfers).

There may also be circumstances in which we need to disclose your personal data to third parties in connection with the restructuring of our business, in which case we will require such third parties to protect your data to the same high standards set out in this policy.

5. HOW LONG WE STORE PERSONAL DATA FOR

We only retain personal data for as long as is necessary for the specific purpose(s) it was collected for (or for related compatible purposes such as complying with applicable legal, accounting, or record-keeping requirements).

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from its unauthorised use or disclosure, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

6. HOW WE KEEP PERSONAL DATA SAFE

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, damaged or destroyed, altered or disclosed. This includes both physical security measures (such as keeping paper files in secure, access-controlled premises) and electronic security technology (such as digital back-ups and sophisticated anti-virus protection).

We limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to legal and contractual confidentiality obligations.

We have put in place reporting procedures to deal with any suspected personal data breach and will notify you and any applicable supervisory authority of a breach when we are legally required to do so.

7. INTERNATIONAL TRANSFERS

We normally only store personal data within the European Economic Area (**EEA**). However, some of the technology and support services we use are provided by

international organisations and/or companies which are based outside the EEA. We may also share your personal data within the NRI group of companies, which will involve transferring it to Japan and other countries outside the EEA.

Before using such service providers or making such transfers to NRI group companies outside the EEA, we take steps to make sure that any personal data they process is adequately protected and transferred in accordance with Data Protection Laws, usually by one or more of the following methods:

- ensuring the recipient is in a country which the European Commission has deemed provides adequate protection for personal data;
- implementing appropriate safeguards such as requiring the recipient to enter into Standard Contractual Clauses approved by the European Commission; or
- (if the recipient is based in the USA) transferring personal data to recipients who are certified under the EU-US Privacy Shield scheme.

If you would like more detailed information on the measures and safeguards which we implement for such data transfers, then please contact us using the details set out in section 1 above.

8. YOUR RIGHTS AS A DATA SUBJECT

Data Protection Laws provide you with certain rights in relation to your personal data. These are as follows:

- **The right to access your personal data.** This enables you to receive a copy of the personal data we hold about you.
- **The right to request correction or completion of personal data**. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **The right to request erasure of your personal data**. This enables you to ask us to delete or remove personal data (though this may not apply where we have a good, lawful reason to continue using the information in question). You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **The right to object to processing of your personal data.** You can object to us processing personal data for legitimate interests purposes or for direct marketing.
- **The right to restrict how your personal data is used**. You can limit how we use your information (primarily to storage or for use in legal claims).
- **The right to have a portable copy or to transfer your personal data**. We will provide you, or (where technically feasible) a third party, with a copy of your personal data in a structured, commonly used, machine-readable format. Note this only applies to automated information we process on the basis of your consent or in order to perform a contract.
- **The right to withdraw consent.** If we are relying on consent to process your personal data you have the right to withdraw that consent at any time.

Responding

We try to respond to all personal data requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or if you have made a number of requests. Please also bear in mind that there are exceptions to the rights above and some situations where they do not apply.

We may need to request additional information from you to help us confirm your identity. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you to clarify your request.

Fees for making a request

You will not normally have to pay a fee to access your personal data (or to exercise any of your other rights). However, we may charge a reasonable fee if your request is unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

How to make a request

If you want to exercise any of the rights described above, please contact us using one of the methods explained in section 1 above.

Your right to complain to a supervisory authority

You have the right to complain to a data protection supervisory authority (which, in the UK, is the ICO) if you are not satisfied with our response to a data protection request or if you think your personal data has been mishandled. For further information on how to make a complaint, please visit https://ico.org.uk.

9. UPDATES TO THIS POLICY

We will update this policy from time to time. The current version will always be posted on our website. This policy was last updated on 27 June 2018.