

Data Protection Information Notice
For Employees and Former Employees

Controller: National Institute for Bioprocessing Research and Training Limited

Introduction

This Notice sets out details of how and why National Institute for Bioprocessing Research and Training Ltd (“**NIBRT**,” “**we**,” “**us**,” “**our**”), and third parties, collect and process personal information in connection with your employment with NIBRT or its affiliates, or associated interactions with us (our **relationship**). We do this in compliance with our obligations under applicable data protection law. This Notice explains what personal data is collected, the purposes for which it is used, the third parties to whom it may be disclosed and how individuals can exercise their rights in relation to their personal data.

About Us

NIBRT is the controller of your personal data as part of our relationship. NIBRT engages third party service providers to process such personal data on our behalf and those third parties act as processors. We are not required to designate a Data Protection Officer. If you have any questions about the use of your personal data, your data protection rights or if you want to exercise those rights, please contact gdpr@nibrt.ie.

Scope

This Notice applies to you, whether you are a current (or former) employee, partner, worker, intern, transition year student, secondee, temporary worker, agency worker, consultant, or individual contractor. It also applies to third parties whose information you provide to us in connection with our relationship with you (for example, in respect of emergency contact information). Please ensure that you provide a copy of this Notice to any third parties whose personal data you provide to us.

Where we refer to 'employee personal data' or 'employment' in this Notice, we do so for convenience only, and this should in no way be interpreted as purporting to confer employment status on non-employees to whom this Notice also applies. This Notice does not form part of any contract of employment and does not confer any contractual right on you or place any contractual obligation on us.

It applies to all personal data collected, maintained, transmitted, stored, retained, or otherwise used (i.e. processed) by us regardless of the media on which that personal data is stored. We may update this Notice at any time and will notify you in writing of any changes.

Personal Data that we Process

'Personal Data' is defined as any data relating to a living individual who can be identified directly from that data or indirectly in conjunction with other information. We hold some or all of the types of personal data set out in Appendix 1, in relation to you.

NIBRT collects personal data relating to you from you or from public sources and in connection with our relationship and in connection with ensuring compliance with our legal obligations. In addition, we may collect personal data relating to you from third party sources such as specialist databases in connection with complying with legislation relating to taxation, and other legislation or from other specialist

databases or sources for vetting or screening purposes or fitness and probity assessments or from employment or previous employers.

Personal data will be processed for the following purposes and on the legal grounds set out below:

Purpose	Lawful Basis
<ul style="list-style-type: none"> • processing your application with us and during the recruitment process, to assess your suitability for a role, establishing your identity and determine the terms on which you work with us and to manage an effective recruitment process; • during our relationship for normal HR management and administration purposes, to ensure that the terms and conditions of your appointment are properly adhered to and managed, to manage the relationship in accordance with relevant policies. • paying you and (where relevant) deducting tax and national insurance and other mandatory or optional contributions; paying you expenses • assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits; • conducting performance reviews, managing performance, and determining performance requirements including decisions about promotions and pay reviews; • making decisions about our relationship, to effectively manage the termination of our relationship and ensuring the termination of our relationship is in accordance with relevant policies; • maintaining appropriate business records; • to ensure network and information security, including preventing unauthorised access to our computer and electronic communications system and preventing malicious software distribution; • education, training, and development requirements; • Providing you with building and IT access • Monitoring use of IT and communications in accordance with our information security policy and standards; 	<p>That it is necessary to take steps at your request prior to entering into our contract with you and for the performance of our contract with you;</p>

<ul style="list-style-type: none"> • Keeping attendance records; • Organising business travel, accommodation, arranging visas and permits, conference and event management including offsites; • Keeping records of gifts and entertainments offered and received; • To provide compensation and benefit plans administration services, and assist NIBRT in discharging essential functions regarding its compensation and benefit plans; and 	
<ul style="list-style-type: none"> • for quality control, business and statistical analysis, market research or for tracking fees and costs or for customer service, training, and related purposes; • administering and monitoring your professional obligations; • use of closed-circuit television (cctv) for security; • use of photographs on our NIBRT websites and NIBRT materials; • use for staff welfare, cultural, sports and social activities; • providing references; • to respond to, evaluate or deal with any queries, complaints, or legal issues in relation to you; • internal and external audits and, where necessary, investigations; • maintaining emergency contact details 	<p>That it is necessary for the purposes of our legitimate interests¹ or the legitimate interests of a third party to whom your personal data is provided. We will not process your personal data for these purposes if our or the third party's legitimate interests should be overridden by your own interests or fundamental rights and freedoms. The legitimate interests pursued by us in this regard include:</p> <ul style="list-style-type: none"> ○ Conducting our business in a responsible and commercially prudent manner and dealing with any disputes that may arise; ○ Preventing, investigating or detecting theft, fraud, or other criminal activity; ○ Pursuing our organisational and social responsibility objectives.
<ul style="list-style-type: none"> • to ensure your health and safety at work, • establishing, exercising, defending or gathering evidence relating to any legal claims, litigation or grievance or disciplinary hearings; 	<p>That it is necessary to comply with our legal obligations;</p>

¹ Legitimate Interest – as defined by GDPR

<ul style="list-style-type: none"> • complying with our legislative and regulatory obligations in connection with our dealings with you, including pension law, revenue law, health and safety law, taxation, crime-detection, prevention, investigation and prosecution, the prevention of fraud, bribery, anti-corruption, tax evasion or equivalent, to prevent the provision of financial and other services to those who may be subject to economic or trade sanctions, in response to legal or court requests or requests from regulatory authorities or where it is in the public interest; • to communicate with you by way of notice pursuant to applicable legislation; • where required for tax reporting purposes; • equal opportunities monitoring; • to afford natural justice and fair procedures (where relevant); 	
<ul style="list-style-type: none"> • to protect your vital interests in the event of an emergency or accident; 	<p>In certain limited circumstances, where we need to protect your interests (or someone else's interests) or where it is needed in the public interest or for official purposes.</p>

In certain limited circumstances, NIBRT may also use the lawful basis of "Consent" to process your personal data.

How we use special categories of sensitive personal data

NIBRT will not process sensitive personal data, unless one of the following circumstances is met;

- Where it is necessary for the purposes of carrying out the obligations and exercising our specific rights or if you are in the field of employment and social security and social protection law;
- Where it is necessary to protect your vital interests or that of someone else where the data subject is physically or legally incapable of giving consent;
- Where it is needed in the public interest, or is requested by a law authority;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
- 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;

- Where you have already made the information public;
- Where NIBRT is subject to a due diligence process and as such provides professional experience details of senior management or key individuals in the business; and
- In certain circumstances with your explicit written consent;

Security and Storage of Personal Data

We securely store your personal data in centralised databases, with controlled access to such databases. Access to personal data (including special data) in both electronic and paper form is restricted to members of the HR Team and employees who have a legitimate and justifiable reason to view such data.

Recipients of Data

Your personal data may be disclosed to various recipients in connection with the above purposes, including:

- The Board of NIBRT and (in circumstances where there is legitimate interest, performance of a contract or legal obligation) other employees, in relation to the HR activities of NIBRT;
- Third parties to assist in the administration, processing and management of certain activities pertaining to past, current and prospective employees e.g., payroll providers, pension and health insurance providers, pensions trustee;
- Individuals or companies employed by NIBRT in respect of business travel, accommodation and event organisation;
- The Revenue Commissioners and other foreign tax authorities as required by applicable law;
- The Department of Social Protection, Pensions Authority, auditors, or other competent governmental or regulatory authorities, trade unions or equivalent industrial relations body and bodies as requested or required by law;
- Regulatory bodies to whom we are obliged or required to disclose information including Workplace Relations Commission, Courts and Court-appointed persons;
- Relevant Government departments and agencies;
- Other third parties who we engage to provide services to us, such as building landlords, professional advisers, independent investigators, insurers, occupational health specialists, legal advisers, auditors, IT service providers and software as a service provider.
- Learning and development providers e.g. professional bodies, external training, conferences organisers;
- Relatives or legal representatives of past, current and prospective employees; and

Transfers Abroad

In connection with the above purposes your personal data may be transferred outside the European Economic Area, including to a jurisdiction which is not recognised by the European Commission as providing for an equivalent level of protection for personal data as is provided for in the European Union. If and to the extent that we do so, we will ensure that appropriate measures are in place to protect the privacy and integrity of such personal data and in particular will comply with our obligations under GDPR governing such transfers, which may include:

- (a) entering into a contract governing the transfer which contains the “standard contractual clauses” approved for this purpose by the European Commission;
- (b) in respect of transfers to the United States of America, ensuring that the transfer is covered by any mechanism approved by both the European Commission and the Federal Government of the United States of America (so long as that it meets with the requirements of GDPR as regards reliance on adequacy decisions under Article 45 of the GDPR);
- (c) transferring your personal data pursuant to binding corporate rules; or
- (d) a transfer where the European Commission has decided that the recipient ensures an adequate level of protection.

Further details of the measures that we have taken in this regard and the territories to which your personal data may be transferred are available by contacting us as set out above.

Retention

We will retain your personal data for the duration of our relationship and for such a period of time as required to satisfy the purpose for which the data was collected and used, unless a longer period is necessary to comply with our obligations under applicable law and, if relevant, to deal with any claim or dispute that might arise. Usually, we retain your data for the duration of your employment with us to a normal maximum of seven years in accordance with our record retention policy.

Your Rights

You have the following rights, in certain circumstances and subject to applicable exemptions, in relation to your personal data:

- the right to access your personal data, together with information about our processing of that personal data;
- the right to rectify any inaccuracies in your personal data;
- the right to have any incomplete personal data completed;
- the right to erase your personal data (in certain specific circumstances).
- the right to request that your personal data is no longer processed for particular purposes (in certain specific circumstances);
- where the legal basis for processing is consent, the right to withdraw your consent at any time;
- the right to object to the use of your personal data or the way in which it is processed where we have determined it to be necessary for the purposes of our legitimate interests;

- the right to data portability (in certain specific circumstances);
- to lodge a complaint with a supervisory authority in the European Member State of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of personal data relating to you infringes the requirements. A list of the relevant supervisory authorities and their contact information is included in Appendix 2.

However, these rights may not be exercised in certain circumstances, such as when the processing of your data is necessary to comply with a legal obligation or for the exercise or defence of legal claims. If you wish to exercise any of your rights in this regard, please contact gdpr@nibr.ie. We will respond to your request within one month. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. We may request proof of identification to verify your request.

What happens if you do not provide us with your information

If we believe that we require relevant information to effectively manage our relationship, we may not be able to continue our relationship with you e.g. process your job application or (in certain circumstances) to pay you or administer your pension if you decline to provide us with that personal data. Where information is needed for a statutory or contractual requirement, then this is set out in the Purpose & Lawful Basis table above and future updates to this Notice.

Changes to this Notice

We reserve the right to update this Notice at any time and an updated Notice will be made available when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

Further Information

We are not required to appoint a Data Protection Officer. If you require any further clarification regarding this Notice, please contact gdpr@nibr.ie.

Appendix 1

General Personal Data

Personal – Recruitment related data and information on your personnel file - these include your name, signature, postal address, nationality, email address, fax number, date and place of birth, nationality, equal opportunities, credit history, signatures, references, work and educational history, right to work documentation, your PPS or social security number (or equivalent); passport number; utility bills, photographic identification and verification such as copies of your passport, passport number, gender, drivers licence and address verification, photographs, working hours, annual leave and other holiday records, emergency contact details, marital status, next of kin and family details.

Professional – Curriculum Vitae and/or application form, previous employment background, references from previous employers, background reference check, directorships, shareholdings, address and identification verification, record of interview/interview notes, selection and verification records, psychometric tests, educational details, professional and/or academic transcripts, professional certifications, special skills including (driver) licenses, language skills, memberships of committees or other bodies;

Employment – work contact details (work email address and telephone number), identification number, photograph, videos, business cards, details regarding the job function, primary work location, start date, working hours, employment status, your terms and conditions of employment or engagement, contract of employment, trade union membership and deductions, notice period, signed confidentiality agreement, immigration status, visa, relocation assistance including taxation, work permit details, job description, history and details of current position;

Premises and IT access – information required to access company systems and applications such as email account and system passwords, login and access records, download and print records, call recordings, records of email and internet usage in accordance with our email and internet policy, CCTV images captured through the legitimate use of CCTV within NIBRT, car type and registration plate.

Fees, remuneration and benefits – fees/payment and benefits package, base salary, bonus, compensation type, long term incentives, long service, pension scheme, PRSA, health insurance scheme (and any third-party beneficiaries), company credit card data, salary reviews;

Travel – Organising business travel, accommodation, arranging visas and permits; passports, visas, dates of travel, flights, car and taxi hire, hotels, meal, dietary requirements, entertainment, credit cards and out of pocket expenses

Leave – including documentation which may be provided in connection with any statutory leave, sick leave, holiday and family related leave records such as maternity, carer's, parental and adoptive, garden leave, and any other type of leave such as study leave, force majeure;

Payroll information – these include your PPS number, bank account details, salary arrangements, bonus entitlements and tax allowances.

Performance, grievance and disciplinary details – these include performance and grievance review forms, notes from performance review and grievance investigation meetings, performance improvement and grievance plan documentation, witness statements, complaints.

Training and development – such as data relating to training and development needs or training received;

General correspondence/meetings – relating to grievance and/or disciplinary processes, misconduct or performance issues, data arising in connection with litigation and complaints, involvement in incident reporting and disclosures;

Health & safety – nature of incident, injuries and remediation;

Incapacity - any accommodations or adjustments in connection with any incapacity.

Legal & regulatory –

- securities trading information including information relating to family members and other accounts under employees' control, details of any shares of common stock or directorships;
- Information about outside activities for employees and family members;
- Information about gifts received/given for the employee and family members; and
- Information about potential conflicts with your family members that impact on your role or with NIBRT in general
- Provision of current staff data to whistleblower service provider.

Information obtained through electronic means – these include emails stored in your email inbox, data relating to your internet browsing history, your use of devices and Apps installed on these devices, your IP address, CCTV footage and other information obtained through electronic means such as swipe-card records.

Medical information and pension details – these include sick certificates, sick leave records, sick pay records, vaccination status, occupational health assessments and pension details.

Termination of our relationship – these include resignation letters, exit interviews and reference letters.

Call recordings – We may collect and process personal data relating to you in connection with our relationship, such as via correspondence and calls, and in connection with our relationship with you. Telephone calls with you may be recorded for the purposes of record keeping, security and training.

Special Categories of Personal Data

Medical information– these include sick certificates, sick leave records, sick pay records and occupational health assessments.

Special categories of more sensitive personal information – information about your race or ethnicity, religious beliefs, sexual orientation and political opinions, membership of a trade union or equivalent industrial relations body, information about your health, including any medical condition, health and sickness records, genetic information and biometric data.