NPD Employee Data Privacy Notice – UK

1. Scope of Notice

This Notice is intended for each employee ("**you**") of an entity controlled by The NPD Group, Inc. ("**NPD, Inc.**"). The controller of your personal data is your employer, and in limited cases your employer and NPD, Inc. (together, "**NPD**"), each acting as an independent and autonomous controller of your personal data.. This Employee Data Privacy Notice ("Notice") sets out which personal data we collect and for which purposes it is processed, as well as other information necessary to ensure fair and transparent processing of personal data when we act as data controller of your personal data, that is, when we determine why your personal data is processed, and how it is processed. Additional details regarding privacy and protection may be found in the NPD Authorized Use Policy and the NPD Information Security Policy and such other polices as NPD may implement, which can be found on NPD's intranet.

Throughout this Notice we use the term

- "**processing**" to refer to all activities involving your personal data, including collecting, handling, storing, sharing, accessing, using, transferring, erasing and disposing of personal data.
- "**personal data**" to refer to information relating to a person who is directly or indirectly identified, such as a name, phone number or one or more factors specific to that individual's physical, physiological, mental, economic, cultural or social identity.
- "**special categories of personal data**" or "sensitive personal data" to refer to information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, ; genetic data; biometric data for the purpose of uniquely identifying a natural person; or data concerning health or a natural person's sex life or sexual orientation, or relating to the commission or alleged commission of a crime.

Summary of Key Information about our Personal Data Processing

Once you are employed by us, we use personal data that you provided as part of the recruitment and on-boarding processes pursuant to our job candidate privacy notice, together with additional personal data we collect throughout the course of your employment (for instance, in relation to performance reviews, participation in benefit schemes, trainings received and disciplinary processes).

The personal data we collect is used primarily for managing our workforce, and complying with employment contracts and applicable law. The personal data is stored and processed in systems in the country where we operate and in the US, where our parent company is established and where there are third party service providers acting on our behalf.

You have certain rights in respect of your personal data, detailed in Section 10 below, which you can exercise by clicking here.

2. Legal Basis and Purposes for Processing Your Personal Data

Your personal data will be processed by NPD, Inc. and its group entities ("Group") for various purposes on the legal bases as set out below:

2.1. Legal Basis for Processing

Whenever NPD processes your personal data, we do so on the basis of a lawful "justification" (or legal basis) for processing. In addition, processing of sensitive data (including data relating to health, sexual life, racial or ethnic origin or religious beliefs and criminal convictions data) is always justified on a separate legal basis.

In the majority of cases, the processing of your personal data will be justified by one of the following legal bases:

- processing is necessary to give effect to your contract of employment (for example, collecting bank account details to pay your salary, creating your access rights, responding to grievances, managing beneficiary details, administering termination);

- processing is necessary for us to comply with a legal obligation (for example, administering benefits schemes, reviewing eligibility for work, creating an employee record (including absences), addressing occupational health issues, managing professional qualifications, managing IT security, disclosing tax data to a government authority or salary information to a national insurance scheme);

- processing is in our legitimate interests as a business and as your employer and our interests are not overridden by your interests, fundamental rights or freedoms (for example, assessing new job opportunities, reviewing your performance at work, managing litigation or other legal requests) and specifically our interests in:
  the effective management and operation of the Group;
  our engagement with our workforce;
  developing our business and the business of the Group;
  increasing the efficiency of our processes and practices;
  striving to ensure compliance with applicable laws and business norms;
  avoiding or mitigating harm to you, to our customers, to us and the Group, and to third parties; or

- processing is based on your prior explicit consent.

The processing of special categories of personal data will also be justified by one of the following:

- processing is necessary for the purposes of carrying out obligations under employment law and/or the applicable national collective bargaining agreements (notably as they relate to insurance and benefit schemes);

- processing is carried out with your explicit consent;

- processing is necessary for the establishment, exercise or defense of legal claims; or

- in exceptional circumstances, processing is necessary to protect your vital interests and you are incapable of giving consent.

In exceptional circumstances, truly voluntary programs (for example, a talent development program or use of your photograph in Group promotional materials) may involve processing based on your freely given and informed consent. If consent is required for the processing in question, it will be sought from you separately to ensure that it is freely given, informed and explicit. Information regarding processing based on your consent will be provided to you at the time that consent is requested, along with the consequences of not providing any such consent. You should be aware that it is not a condition or requirement of your employment to agree to any request for consent from NPD.

2.2. Processing for Human Resources Management

The Group may process your personal data for the purposes of Human Resources Management. This may include processing your personal data for:

a. Management of NPD workforce, including: general management of employees; payroll; hiring; benefits and compensation; determining physical and/or mental fitness for work; reviewing and evaluating employee performance; monitoring attendance; investigating suspected misconduct or non-performance of duties; head count analysis; senior staff succession planning; employee training, appraisal and promotion; employee travel; management forecasting; employee discipline and termination; negotiation with trade unions or other employee representatives; emergency alerts;

b. Management and development of the Group's business;
c. Administration of NPD and Group policies and procedures;
d. Compliance with an obligation imposed by local, national, federal or any other applicable law or regulation;
e. Management of assets and facilities, including security thereof;
f. Providing IT and information processing support and IT applications and systems maintenance;
g. Monitoring IT systems to prevent any use contrary to Group policies and/or criminal or civil offenses;
h. Monitoring and preventing sexual or other unlawful harassment, discrimination and/or criminal or civil offenses where warranted by a specific set of circumstances;
i. Provision of Group services and other services (such as IT and communication systems);
j. Analyzing, preparing or effecting any planned or contemplated structural change or reorganization implicating a Group company, function or department;
k. Analyzing, preparing or effecting any planned or contemplated restructuring, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of any member of the Group;
l. Protecting and defending any Group company's rights and interests (including in connection with any administrative, court, arbitral or mediation proceeding);
m. Preserving or defending any Group company's rights in court, responding to law enforcement requests or discovery procedures, or where required or permitted by applicable laws, court orders, government regulations, or government authorities (including tax and employment);
n. Communicating within the Group and with third parties in furtherance of the foregoing; and
o. Managing, updating, storing, archiving and deleting personal data in support of the Group's activities related to any of the foregoing purposes.

2.3. Establish, Exercise and Defend Legal Claims

The Group may process your personal data (including special categories of personal data) for the purposes of establishing, exercising and defending potential legal claims.

Your personal data is processed for this reason on the basis of the Group's legitimate interest in processing your personal data for these purposes in order to be able to establish, exercise and/or defend potential legal claims in the event of a dispute or controversy between you and NPD, or between a Group entity and a third party, which may be related to or implicate your employment, as well as in the context of organizing or conducting internal investigations, or in connection with government or law enforcement.

Group entities that may process your data are listed on our website at https://www.npd.com/wps/portal/npd/us/about-npd/offices/.

3. Types of Personal Data Processed

NPD processes different types of your personal data, depending on your role, your location and the terms and conditions of employment relevant to you. Typically the categories of personal data we process will include the following:

- Contact information (such as your name, user name, address, email address and phone number);
- Date of hire or re-hire;
- Nationality;
- Place and date of birth;
- Driver's license number, social security number, social insurance number, national ID, tax number and other governmental identifiers;
- Gender;
- Marital status;
- Disability status;
- Military status;
- Psychometric and ability test results;

- Information relating to job positions (such as your employee ID, job title, company, department number, supervisor, business phone and business email, standard hours, performance ratings);
- Training courses;
- Emergency contact details;
- Payroll information, including salary, compensation, benefits information, including bank details and payroll frequency;
- Payment information;
- Pension arrangements, medical insurance arrangements, life assurance arrangements and details of beneficiaries, if any;
- Absences and leaves;
- Information relating to benefits, if any;
- Information relating to expenses, if any;
- Experience information (such as your resume information and summary of employment history and educational background, skills, records and appraisals, and statements of opinion or intention);
- Use of NPD assets and facilities;
- Employment documents, including but not limited to copies of employment contracts, IDs, birth certificate, educational degrees, medical checks, criminal checks;
- Termination data, such as date of and reason for cessation of employment and post-employment contact information (if applicable); and
- Logging and other records of communications within the Group and with third parties in furtherance of the purposes set forth in Section 2. above.

Apart from personal data relating to yourself, your friend and family data (such as emergency contact and beneficiary details) will be processed by NPD solely if you provide it to your employer and in order for your employer to contact them when necessary. You are required to provide any such friends and family with a copy of this Notice and, where required, obtain their consent.

4. Sources of Personal Data

The personal data we process about you will have been provided by you, either during your application for employment, the employee on-boarding process, or on an ad hoc basis during the course of your employment.

You will usually provide the personal data directly to your managers or local Human Resources contact or enter it into our systems (for example, through your self-service access to Workday, your participation in Human Resources processes, emails you send or through verbal information which may be recorded).

During the recruitment process, we may request references from third parties, and carry out screening and vetting processes using third party sources, and retain that personal data after you have been employed (where permitted by applicable law).

We also receive information which may include your personal data from your manager (for example, in respect of performance reviews), from Human Resources, or, from time to time, from other colleagues (for instance, in the course of conducting a disciplinary investigation).

From time to time, we may receive personal data about you from other third parties (for example, customers, business partners or regulatory bodies), medical reports from external professionals, tax authorities, or benefit providers.

In some circumstances, personal data may be collected indirectly from monitoring devices or by other means (for example, building and location access control and monitoring systems, Closed Circuit TeleVision, telephone logs and recordings and email and Internet access logs), if and to the extent permitted by applicable laws.

5. Processing Your Personal Data

The Group is committed to ensuring that all employee personal data is:

- Processed fairly and lawfully;
- Processed for specific purposes only, and not in any manner incompatible with those purposes;
- Adequate and relevant;
- Kept accurate;
- Retained no longer than necessary;
- Processed consistent with your rights; and
- Kept secure.

In some cases, providing your personal data is necessary to enter into your employment contract with us, or to comply with applicable law. If you do not provide us with such information, we may not be able to perform our contract with you. We will inform you when providing your personal data is necessary and what the impact will be on your relationship will be if you do not provide it. For example, if you do not provide us with your bank details, we will not be able to pay you. In some cases it may mean that we are unable to continue with your employment or engagement because NPD will not have the personal data we believe to be necessary for the effective and efficient administration and management of our employment relationship with you.

6. Sharing Your Personal Data with Third Parties

Where required in order for your employer to perform its obligations to you, or for you to perform your job function, or for the purposes described in this Notice, your employer will share your personal data with other Group entities, third party service providers who maintain reasonable security practices commensurate with applicable law, government agencies and/or other third parties, such as Group customers. In some cases, third party service providers may be granted access to a specific Group database, but their access is restricted on a need-to-know basis via access limitations. Group entities and third parties with whom your data will be shared include:

- The NPD Group, Inc.;
- your employer's bank and payroll processor;
- applicable tax, social security and employment authorities, and mandatory fund administrators;
- third party insurance and benefits providers (where applicable);
- NPD HR and IT personnel responsible for HR management or IT processing and security functions;
- third parties providing IT services and support for any of the purposes described in Section 2. above;
- financial consultants, professional advisers and in-house and outside counsel;
- educational institutions which you attend;
- employment agencies;
- external training providers; and
- where permitted by law and required as a part of your job function, Group customers or vendors or other third parties where this is helpful to developing the business (for example, to compete for, or meet obligations under, an existing or possible business contract).

We may provide data to a third party if we believe in good faith that we are required to so for legal reasons or that this is necessary to prevent harm or injury to us, our staff, users or members of the public or if we need to do so to defend our legal rights. For example, we may provide personal data if we are ordered by a court to do so.

Wherever required under applicable law, the relevant Group company will enter into with third party service providers data processing or similar agreements that require in particular that such third party service providers maintain the same level of personal data protection as implemented by the Group. Where these third parties act as a "data processor" they carry out their tasks on our behalf and upon our instructions for the purposes stated in this notice.

7. Transfers of Personal Data Outside of Your Country

Your personal data (as described in Section 3. above) may be transferred to other Group entities or to third parties described in Section 5. above, only to the extent required for your employer to perform its obligations to you, or for you to perform your job function, or for the purposes described in this Notice. In particular:

- Your professional profile and contact information contained in systems such as Outlook, SharePoint, and Workday, will be accessible to all employees of Group companies worldwide.

- Your personal data may be transferred to Group headquarters in the U.S. and/or to Group employees located inside or outside your country, including countries outside EU/EEA and/or to a person or company that is not part of the Group located in or outside your country, on a need-to-know basis. In some cases, transfers of your personal data may be made to countries that are considered by the European Commission or by other governmental entities or authorities to offer adequate protection for personal data. In other cases, transfers may be made to countries, like the U.S., that are not considered to offer adequate protection for personal data; transfers to those countries outside the EU/EEA will be made pursuant to the standard contractual clauses approved by the European Commission, the EU-U.S. Privacy Shield certification, Binding Corporate Rules, or other safeguards that ensure an adequate level of protection where legally permissible.

Where applicable, you are entitled, upon request to your Human Resources manager, to receive information concerning the appropriate safeguards (for example, Standard Contractual Clauses) that have been taken to protect your personal data in relation to such transfer.

- Transfers may be made to respond to law enforcement requests or discovery procedures, or where required or permitted by applicable laws, court orders, government regulations, or government authorities (including tax and employment). Such transfers may entail access by courts or governmental authorities outside your country, after having ensured that only your minimal necessary data is disclosed and transferred, or that such data is de-identified or that, where possible, appropriate stipulative court orders have been issued.

8. Data Security

Your personal data will be secured by taking security measures that are commensurate with the sensitivity of the personal data processed. To this end, the Group maintains reasonable physical, technical, and administrative security measures (including lawful IT system monitoring) with a view to protecting employee personal data against theft; accidental loss; unauthorized alteration; unauthorized or accidental access, processing, erasure, use, disclosure or copying; and/or accidental or unlawful destruction.

9. Data Retention

The Group keeps employee personal data only for as long as is required to satisfy the purpose for which it was collected by us or provided by you including for the duration of the applicable statute of limitations, which may surpass the term of your employment. In certain cases, legal or regulatory obligations require us to retain specific records for a set period of time, including following the end of your employment.

We maintain a retention policy which we apply to records in our care. In all cases, where your information is no longer required we will ensure it is disposed of in a secure manner and, where required by applicable law, we will notify you when such information has been disposed of.

10. Updating Employee Personal Data and Your Rights

- Right to Correct (Rectification) - you are entitled to have any inadequate, incomplete or incorrect personal data corrected (that is, rectified). You also have a responsibility to ensure that changes in personal circumstances are notified to NPD so that we can ensure that your personal data is up-to-date.

- Right to Access - you have the right l to request access to your personal data and additional information about the processing of your personal data.

- Right to Withdraw Consent - in the event your personal data is processed on the basis of your consent, you have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- Right to Erasure - you are entitled to have your personal data erased under specific circumstances, such as where you have withdrawn your consent, where you object to processing based on legitimate interests and we have no overriding legitimate grounds (see below) or where personal data is unlawfully processed.

- Right to Data Portability - where we are relying (as the legal basis for processing) upon your consent, or the fact that the processing is necessary to perform a contract to which you are party or to take steps at your request prior to entering a contract, and the personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to NPD in a structured, commonly used and machine-readable format, and also to require us to transmit it to another controller where this is technically feasible.

- **Right to object to processing (including profiling) based on legitimate interest grounds - where we are relying upon legitimate interests to process personal data, you have the right to object to that processing. If you object, we must stop that processing unless we can demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms, or we need to process the personal data for the establishment, exercise or defense of legal claims. Where we rely upon legitimate interest as a basis for processing we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.**

- Right to Restriction –- you may object to further processing of your personal data in the following circumstances:

a. where you object to the accuracy of your personal data, until we have taken sufficient steps to correct your personal information or verify its accuracy;

b. where the processing is unlawful but you do not want us to erase the personal data;

c. where NPD no longer needs your personal data for the purposes of the processing but you require such personal data for the establishment, exercise, or defense of a legal claim;

d. where you have objected to processing based on legitimate interest grounds, pending verification as to whether NPD has compelling legitimate grounds to continue processing.

Should your personal data be subject to restriction (which means that we will only store the data), we will only process restricted data with your consent or for the establishment, exercise or defense of legal claims.

- Right to Lodge a Complaint - You have the right to lodge a complaint with the supervisory authority of your habitual residence, place of work or place of alleged infringement. The supervisory authority in the UK is the ICO.

Your right of access, correction, deletion, blocking and objection, and your responsibility to notify changes in your personal circumstances, as well as any other right you may have under applicable law, may be exercised as follows:

a. General requests may be made by clicking **here**.
b. You can update selected data about you by logging into Workday.

To obtain further information regarding your rights, to exercise any of your rights, or to ask any questions regarding the processing of your personal data, please click **here**.

11. Changes to this Notice

Any changes or updates we may make to this Notice will be posted in advance **here**. We will notify current employees in advance via internal communications about any changes to this Notice that are material or may impact you. For other changes, please check back frequently **here** to see any updates or changes to this Notice.

I ACKNOWLEDGE THAT I HAVE READ AND UNDERSTOOD THIS NOTICE AND I AGREE TO COMPLY WITH THIS NOTICE AT ALL TIMES.

Issued: May 2018
A copy of this notice is available in the "Reviewed Documents" section of Workday that NPD employees can access.