



## NPD Employee Data Privacy Notice - CANADA

### 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”). This Notice sets out relevant information regarding the privacy and protections accorded to your personal data by or on behalf of NPD. Additional details regarding privacy and protection may be found in the NPD Authorized Use Policy and the NPD Information Security Policy and such other policies as NPD may implement, which can be found at <https://npdinsider.npd.com/wps/myportal/npdintra/insider/it-ops/information-security/policies/>. When used in this notice, the term “personal data” means any data that directly or indirectly identifies an individual, such as a name, phone number or one or more factors specific to that individual’s physical, physiological, mental, economic, cultural or social identity.

### 2. Purposes of Processing Your Personal Data

Your personal data will be processed by NPD, Inc. and its group entities (“Group”) for various purposes to the extent required by or permissible under applicable law, including but not limited to:

- a. Management of NPD workforce, including: general management of employees; payroll; hiring; benefits and compensation; 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.

Your personal data will be processed by NPD, Inc. group entities by electronic means as well as by organized filing systems of hardcopy documents. The provision and the processing of your personal data as outlined above is mandatory. If personal data is not provided, or if you object to the processing of your personal data, it is likely that NPD will not be able to manage the employment relationship between you and your employer.

### 3. Types of Personal Data Processed

NPD processes different types of your personal data, to the extent permitted under applicable laws:

- 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;
- 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.

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.

Sensitive personal data generally will not be processed, except to the extent necessary or authorized under applicable law or if you decide to provide sensitive personal data to your employer; where required, sensitive personal data will be processed only with your express consent, which you may withdraw at any time. When used in this notice, the term "**sensitive personal data**" means information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and health or sex life.

### 4. 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.

Where required by applicable law or internal Group policies, your consent will be requested before processing your personal data. In the event any such consent is sought, you will also be provided with an option to opt-out of the consent so given, and you may withdraw your consent at any time.

## **5. Sharing Your Personal Data with Third Parties**

Where necessary 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; 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).

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 will maintain the same level of personal data protection as implemented by the Group.

## **6. Transfers of 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 necessary 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, 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 to personal data. In other cases, transfers may be made to countries, like the U.S., that are not considered to offer adequate protection of personal data; transfers to those countries will be made pursuant to the standard contractual clauses

approved by the European Commission, relevant national equivalents thereof, or other safeguards where permissible. This means that your personal data may be accessed by law enforcement or regulatory authorities according to the applicable laws of those countries.

- 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.

## **7. 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 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. The Group takes reasonable steps to confirm that third parties who are recipients of personal data have data security procedures in place that are commensurate with those of the Group.

## **8. Updating Employee Data**

You have the responsibility to ensure that changes in your personal data are notified to your employer to be sure that all your data is kept up to date. You have the right under applicable law to access and correct personal data concerning you, subject to limited exceptions that may be prescribed by applicable law. Where justified and allowed by applicable law, you may also require that your personal data be deleted or blocked, or you may be entitled to object to further processing of your data.

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 by signed request or email as follows:

- a. General requests may be made to your local HR department.
- b. You can update selected data about you by logging into Workday.

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

*Issued: March 2017*

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