INFORMATION MEMORANDUM ABOUT PERSONAL DATA PROCESSING FOR NTT EUROPE GDC EMPLOYEES AND CANDIDATES

according to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL as of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, referred to as "GDPR") as amended (hereinafter "Information memorandum").

We would like to provide you with clear and comprehensible information in this Information Memorandum on how we process your personal data, their categories, the scope and purpose for which they are processed, the source from which the personal data are collected and the persons who are your personal data transferred to. You will also find information about your rights in the area of personal data processing.

Table of contents

Version 2019 – v.02, date 28-06-2020.

Who we are and how you can contact us?

NTT Europe GDC s.r.o., located on Pikrtova 1737/1a, Nusle, 140 00 Prague 4, VATIN: CZ06247377, kept by the Municipal Court in Prague with a file number C 278833 (hereinafter "NTT EU GDC"), is a controller of your personal data, which means that it determines the purpose and means of processing personal data, carries out the processing of personal data and is responsible for it. In some cases, NTT EU GDC may also be in the position of a personal data processor, i.e. it processes personal data for purposes specified by another controller. More information about our activities and our services can be found on the website [https://hello.global.ntt/en-us/about-us]. If you do not find answers to your questions in this information memorandum or on our website, or would like to explain some of the information in more detail, you can contact us:

By e-mail: dpo.gdc.cz@global.ntt

By post: NTT Europe GDC s.r.o.

Pikrtova 1737/1a

140 00 Prague 4

Czech Republic

You can also contact our Chief Protection Officer Tomas Jecminek by e-mail: dpo.gdc.cz@global.ntt.

Personal Data Protection Principles

NTT EU GDC is committed to:

- processing your personal data fairly, lawfully and in a transparent manner;
- only collecting personal data from you or a third party for specified explicit and lawful purposes and not processing your personal data which is in any way incompatible with those purposes;
- telling you how we use your personal data either directly or in this Information Memorandum;
- doing our best to ensure that your personal data is adequate, relevant and not excessive for the purpose for which we collect it;
- keeping your personal data accurate, and where necessary, up to date, and taking reasonable steps to ensure that personal data that is inaccurate is erased or corrected without delay;
- keeping your personal data secure through the use of appropriate physical, technical, and organizational measures and limiting access to individuals who have a legitimate business need to access it;
- processing or keeping your personal data for only as long as it is necessary and consistent with the purpose for which it is processed, subject to applicable law;
- ensuring that you know how to and have access to your personal data (unless we are unable to provide access for legal reasons or because your personal data no longer exists); and
- ensuring that any third parties with whom we share your personal data are contractually obliged to comply with applicable privacy laws and implement appropriate physical, technical, and organizational measures to protect personal data.

Legal basis on which we rely to process your personal data

When we process your personal data in connection with the purposes set out in this Information Memorandum, we may rely on one or more of the following legal bases, depending on the purpose for which the processing activity is undertaken.

- Our legitimate interests (or those of a third party with whom we share your personal data) for the purpose of managing and operating our business and for other business and administrative

purposes, except where such interests are overridden by your interests or fundamental rights or freedoms which require protection of personal data.
- We will not process your personal data where your fundamental rights or freedoms override our legitimate interests.
- To perform a contract to which you are a party (for example, your employment contract) or in order to take steps at your request prior to entering into a contract with you.
- Where this is necessary to comply with a legal obligation on us.
- To protect the vital interests of any individual (for example in a medical emergency).
- Where you have granted a consent (for example, where we wish to use your photo for a staff publication).

You can always withdraw your consent. You can withdraw your consent to all processing of for individual purposes of your choice (to which you have given your consent). You can withdraw your consent by sending an e-mail to dpo.gdc.cz@global.ntt .

What types of personal data do we collect and process?

We collect personal data from you in order for us to fulfil our obligations to you as part of our employment relationship with you and as required by law. If you do not provide your personal data, we may be unable to do so.

The type of personal data that we collect depends on the purpose for which we collect it, the surrounding circumstances, your position and any legal or regulatory obligations we are subject to.

Personal data we collect may include the following:

Recruitment and selection: When you apply for a job with us (including when you already work for us and are changing roles), you will be asked to provide personal data to support your application and to enable us to determine your suitability to work for us. This may include the following personal data:

- your name, home address, email address, telephone number, job title, day of birth, gender, marital status, family, nationality;
- your CV, cover letter and any documents in support of your job application, or as part of the recruitment process;
- information relating to any previous job applications you have made to us and/or any previous or existing employment with us;
- information obtained from third parties, including third-party placement firms, recruiters, or job-search websites, as part of the job application and recruitment process;
- interview notes, work visas, results of pre-employment checks, including criminal record checks, credit and fraud checks;
- current and previous employment information (including salary, bonus and benefits);
- information obtained from your referees and/or your previous employer;
- educational qualifications and achievements;
- video/photos or audio recordings that you may submit to us in connection with your job application;
- immigration status and work permit;
- job preferences such as willingness to travel and/or to relocate;
- letters of offer and acceptance of employment and your employment contract;
- camera recordings from cameras located at DDGDCE headquarters.

If you become a NTT EU GDC employee, any personal data provided to us may form part of your employee record.

Employment relationship: To the extent consistent with local privacy laws and regulations, we collect your personal data to administer and manage our employment relationship with you. Personal data we collect may include the following:

- your name, home address, email address, telephone number, date of birth, marital status, nationality, gender;
- photographs, passport and/or driver's license details;
- emergency contact information;
- payroll and benefits information including bank account details, national insurance or birth identification number;
- employee identification number;
- computer or facilities access and authentication information, identification codes, passwords, answers to security questions;
- recordings, video, images;
- camera recordings from cameras located at NTT EU GDC headquarters;
- mandatory policy acknowledgement sign-off sheets;
- forms relating to the application for, or in respect of changes to, employee health and welfare benefits; including short- and long-term disability, medical and dental care;
- health information, criminal records;
- length of service information, leave requests and absence information;
- performance ratings, leadership ratings, targets, objectives, records of performance reviews, records and/or notes of one to ones and other meetings, personal development plans, performance management plans, correspondence and reports;
- interview/meeting notes or recordings and related correspondence;
- vehicle registration and insurance details for work travel.

Sensitive Personal Data

We may collect sensitive personal data such as your birth number, data concerning your health, biometric data or your criminal records for any of the following purposes (as applicable):

- where we are required to do so by applicable law. For example, to comply with applicable employment, social security and social protection laws, including diversity and equal opportunity reporting requirements;
- under a collective agreement between NTT EU GDC and employee representatives, within the scope of relevant employment law;
- to assess your ability to work in the event of sickness or injury;
- necessary to establish, exercise or defend legal claims;
- with your explicit consent.

Access to your sensitive personal data is strictly limited to those employees and external processors with a legitimate business reason for accessing it.

How do we collect your personal data?

We collect your personal data, either directly from you, third parties or from publicly available sources. Where we collect your personal data from third parties, we will take reasonable steps to ensure that those third parties are legally permitted to disclose your personal data to us.

When we collect personal data from you, we always inform you whether the provision of personal data is a legal or contractual requirement or a requirement to be entered into the contract. We also inform you whether you are obliged to provide personal data to us and the possible consequences of not providing them. Your personal data we collect from:

You, mainly:

- based on your requests, inquiries and contract negotiations;
- from telephone communication;
- from e-mail or other written (chats via social media such as LinkedIn, Facebook) communication;
- from personal communication at our branch or other places.

Third parties, mainly from:

- Personnel agencies;
- Your previous employer;
- Your referees;
- Government agencies in the performance of our legal obligations or under special legal regulations.

Publicly available sources, mainly from:

- Social media such as LinkedIn and Facebook;
- Central Execution Register;
- Public Register;
- Trade Register;
- Business Register.

For what purposes do we process your personal data?

We process your personal data only to the extent necessary for the given purpose and for the time necessary to fulfill the purpose. After fulfilling the original purpose (such as fulfilling the contract), we may process personal data for other purposes (such as fulfilling the legal archiving period). The processing purposes are given later in this section. In general, we store your personal information for a period of time determined by law, contract, or based on our legitimate interest (for example, for the duration of the statute of limitations when we may be interested in claiming or defending our legal claims).

We may use your personal data for the following purposes:

Recruitment and selection:

a) identifying and contacting you throughout the job application and recruitment process;
b) processing your job application and determining your suitability for current roles with us;
c) processing details of your employment with us (if successful);
d) verifying information provided by you, or third parties, including identity, qualifications and references;
e) conducting pre-employment background checks, screening and assessments if we employ you including criminal record checks (as permitted by law) and right to work checks;
f) assisting you to obtain work visas and permits if we employ you;
g) making offers and providing contracts of employment;
h) performing administrative functions (e.g. maintaining a repository of correspondence between us and you);
i) enabling us to search our internal databases to help us fill job vacancies;
j) informing you about current or potential job opportunities with us if you request this information;
k) matching your profile against current roles with us;
l) analyzing our job applicant pool in order to better understand who is applying for roles at NTT EU GDC and how to attract top talent;
m) entering your details in our databases to receive future mail and alerts about our job vacancies and events where you have registered to do so. You may opt out of receiving these communications at any time by contacting us at Queries@dimensiondata.com;
n) improving our job application and recruitment process.

Legal ground for these purposes is a legitimate interest in human resources management according to Article 6(1)(f) of GDPR and a consent in the case of m) of previous paragraph according to Article 6(1)(a) of GDPR.

Based on the titles, we process your personal data using non-complicated methods (no profiling).

Employment relationship:

a) establishing, managing or terminating your employment;
b) administering payroll and benefits, including making salary payments, pension deductions, tax withholdings and national insurance contributions;
c) communicating with you and facilitating communication between you and other people;
d) establishing who your emergency contacts are (such as next of kin);
e) compiling staff directories;
f) resource and succession planning and workforce management;
g) budgeting and financial planning;
h) staff development, education, training and certification;
i) project management;
j) performance management;
k) dispute resolution, including carrying out internal reviews, grievances, investigations and audits;
l) business travel and expense management;
m) business reporting and analytics;
n) administering flexible work arrangements;
o) administering employee enrolment and participation in activities and programs offered to eligible employees, including matching donations to non-profit organizations, and health and wellbeing activities;
p) reporting of work-related injuries and illness;
q) managing of employee health and safety and disabilities including absence from work;
r) compliance reporting, including conflict of interest and gifts and hospitality reporting;
s) risk management;
t) processing work-related claims (such as workers' compensation, personal injury and insurance claims);
u) gathering evidence for disciplinary action or termination;
v) complying with applicable laws including employment laws;
w) establishing, conducting or defending legal proceedings.

Legal ground for these purposes is a fulfillment of a contract according to Article 6(1)(b) of GDPR, legitimate interest according to Article 6(1)(f) of GDPR, a consent according to Article 6(1)(a) of GDPR and the fulfillment of legal obligation according to Article 6(1)(c) of GDPR.

Based on the titles, we process your personal data using non-complicated methods (no profiling).

Security purposes: Monitoring communications

NTT (collective term for NTT, Inc. and its affiliates) and NTT EU GDC provide communications services, equipment, and facilities including email, instant messenger, land lines, VOIP and mobile phones to you for NTT business. Your use of these services, equipment and facilities, whether on-site or remotely, must be in accordance with NTT policies, including NTT's Group Acceptable Use Policy and Group Information Security Policy.

Subject to local laws or regulations, we may block access to certain websites, and monitor, record and analyze your use of the communications services, equipment and facilities that we provide to you for NTT business for system, network and data security purposes, including scanning for possible malware and illegal or offensive material. We will also record numbers dialed and the duration of all calls for billing purposes. Where you call one of our internal help desks, those calls may also be recorded for training and quality purposes.

Security purposes: Physical access control

Depending on your role and location, you may require access to various NTT and/or third party locations, facilities, infrastructure, property and records. For NTT locations, prospective, present and past NTT employees, contractors or agency staff and all other workers who have an employment relationship with NTT EU GDC are given an electronic access card which contains their name and photograph ("NTT Pass Card") and in some locations, NTT uses biometric access control systems such as fingerprint access control systems to enable access to those locations, and to ensure site security (not in the case

of NTT EU GDC facility). This information is stored on secure IT systems. Use of the NTT Pass Card and biometric access control systems may be monitored for security purposes and may be used in any investigation by NTT of a suspected crime or serious disciplinary offence and/or law enforcement or other appropriate government or legal agency or authority. Your personal data may also be required by third parties if you need access to third party locations, facilities, records, property and/or infrastructure to do your job.

Security purposes: CCTV monitoring

At NTT EU GDC facility we use CCTV to monitor and enhance the security of our premises and property to deter theft, vandalism, damage or destruction, and to protect our people and third parties.

CCTV records may be shared with third parties, including law enforcement or other appropriate government or legal agency or authority where a suspected crime or serious disciplinary offence has been committed or such disclosure is otherwise necessary to comply with applicable law.

Security purposes: Covert monitoring

In exceptional circumstances, and subject to local laws and regulations, where we have reasonable grounds to believe that suspected criminal activity, (e.g. stealing NTT EU GDC or NTT property), or a serious disciplinary offence has been committed, we may carry out covert monitoring without the suspected individual or individuals being aware that this is the case, and where information cannot be obtained effectively by other non-intrusive means. Covert monitoring may involve electronic, video or audio systems or use of any other information we may lawfully have about the individual or individuals being monitored. Such monitoring will only be carried out as part of a specific investigation.

Information Technology ("IT") administration

To enable you to access and effectively use NTT or a third party's IT systems in order to do your job, NTT and/or third parties may need access to your personal data for the following purposes:

- IT systems access authorization, administration and control (including termination of access) and use monitoring;
- IT fault reporting, management and resolution or with respect to other IT issues you may have when doing your job;
- Systems administration, support, development, testing, management and maintenance.

Legal and regulatory

To comply with our legal and regulatory obligations.

If you do not provide us with your personal data, we may be unable to comply with our obligations to you arising out of our employment relationship with you.

How do we process your personal data and how are they secured?

We are fully aware of the importance of protecting personal data and privacy of our employees and candidates. When processing personal data, we always proceed in such a way that your personal data is well secured and cannot be misused.

We process your personal data only for specified lawful purposes. We keep your personal data secure through the use of appropriate physical, technical, and organizational measures and limit access to individuals who have a legitimate business need to access it.

We took all measures that all processors of your personal data will maintain the confidentiality of all facts, information and data (personal or other) that they have learned in the course of their work. We have concluded a written agreement on the processing of personal data with all processors, where we emphasize the security of your personal data.

Sharing your personal data

We will only share your personal data when we have a legitimate business need or legal obligation to do so. Where we need to do this, we will do so in line with this Information Memorandum and applicable law.

We may share your personal data for the purposes stated in this Information Memorandum (as applicable) with:

- authorized NTT EU GDC personnel including P&C, finance and IT personnel, and other administrative staff, to administer your employment with us, including our obligations under your employment contract, (such as paying you, and providing your employee benefits); as well as providing specialist support to management;
- NTT affiliates and subsidiaries (for example where you are moving roles within NTT). A list of our affiliates is available here.
  NTT ltd. is the party responsible for the management of jointly-used personal data;
- agents and professional advisers of NTT including legal advisers in connection with legal proceedings, to obtain legal advice, or to protect NTT's legal rights;
- auditors and investigators in connection with NTT internal and external audits and investigations;
- third party placement firms, recruiters, or job search websites when you are applying for a position with us;
- authorized personnel of third party suppliers including companies who perform background checks. These companies may be based in another country to where your personal data is collected, and may obtain personal data from other countries where you have lived, worked or studied;
- service providers to provide operational services or facilitate transactions on our behalf, including but not limited to providing us with P&C, finance and administrative services, IT support and data analytics;
- any court, tribunal, governmental or regulatory authority or law enforcement agency with jurisdiction over NTT EU GDC or to comply with applicable laws and regulations;

We may share your personal data in the following situations:

- in response to a request for information by a competent authority in accordance with, or required by any applicable law, regulation or legal process;
- where necessary to comply with judicial proceedings, court orders or government orders;
- to protect the rights, property or safety of NTT, its business partners, you, or others, or as otherwise required by applicable law;
- in connection with any joint venture, merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of our business by or to another company;
- where you consent to the sharing of your personal data.

Any third parties with whom we share personal data are contractually required to comply with applicable privacy laws, to implement appropriate data protection and security measures to protect personal data and are only permitted to use personal data for the purpose for which they are provided with or given access to personal data.

Security

NTT EU GDC is committed to protecting your personal data from accidental or unlawful destruction, loss, alteration, unauthorized access or disclosure by using a combination of physical, administrative and technical safeguards and contractually requiring that third parties to whom we disclose your personal data do the same.

We also limit access to your personal data to only those people with a legitimate reason to access it. We expect that you will assist us to do this by ensuring that you keep your personal data and that of your co-workers and third parties secure.

Cross-border transfers

NTT EU GDC is a subsidiary of NTT which is a global company. We may transfer your personal data to countries where we do business in connection with the purposes identified above and in accordance with this Information Memorandum.

For individuals in the EEA or Switzerland, where we transfer your personal data from a location within the European Economic Area (the "EEA") or Switzerland to a country outside the EEA or Switzerland and that country does not provide a level of protection for personal data which the European Commission ("Commission") deems adequate, we use and adhere to the standard contractual clauses ("SCCs") approved by the Commission, to legitimately transfer personal data. You may obtain a copy of these measures by contacting us as set out in the "Who we are and how you can contact us?" section above.

Retaining your personal data

We will retain your personal data for as long as it is necessary to fulfil the purpose for which they were collected unless a longer retention period is required to comply with legal obligations, resolve disputes, protect our assets, or enforce agreements. The criteria we use to determine retention periods include whether:

- we are under a legal, contractual or other obligation to retain personal data, or as part of an investigation or for litigation purposes;
- personal data is needed to maintain accurate business and financial records;
- there are automated means to enable you to access and delete your personal data at any time;
- the personal data is sensitive personal data in which event we will generally retain this for a shorter period of time;
- you have consented to us retaining your personal data for a longer retention period, in which case, we will retain personal data in line with your consent.

What rights do you have?

We process your data in a transparent way. You may use the following rights at any time during the processing of your personal data:

i. The **right to access** your personal data and to have a copy of the personal data we process.
ii. The **right to rectify** inaccurate personal data we hold about you without undue delay, and taking into account the purposes of the processing, to have incomplete personal data about you completed. We do our best to ensure that the personal data we hold about you is kept accurate and up to date. We ask that you assist us to do this by correcting or updating your personal data, (as applicable) through Workday.
iii. **Right to be forgotten**. You may require us to erase your personal data, and we will do so if:
    - personal data are not necessary for the purposes for which they were collected or otherwise processed;
    - you withdraw your consent to the processing of personal data and there is no other legal reason for the processing;
    - you object to a processing based on a legitimate interest and there are no overriding legitimate reasons for processing, or if you object to the processing of personal data for direct marketing purposes;
    - personal data are processed unlawfully;
    - personal data must be erased in order to fulfill a legal obligation established in the law of the European Union or Czech Republic; or
    - it is the child's personal data collected in connection with the offer of the information society service.

Please note that your personal data cannot be erased if processing is necessary:

- for the exercise of the right to freedom of expression and information;
- to fulfill a legal obligation requiring processing under the law of the European Union or the Czech Republic, or to carry out a task carried out in the public interest or in the exercise of official authority;
- for public interest reasons in the field of public health;
- for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes; or
- for the determination, exercise or defense of legal claims.

iv. **Right to restrict** the processing of your personal data. You may also require us to restrict the processing of your personal data, if:

- the personal data processed are inaccurate;
- the processing is unlawful;
- the personal data processed are not needed for the purposes for which they were collected or otherwise processed; or
- you object to processing.

If you exercise your right to restrict processing and any of the above conditions are met, we will record this fact in our systems, and we will not process such data actively.

If the reasons concerning the restriction of the processing cease to exist, we will remove the restrictions. We will inform you in advance about this situation.

v. **Right to data portability**. Right to receive your personal data from us in a structured, commonly used and machine readable format and to transmit your personal data to a third party without obstruction.

vi. If you believe that there is a breach of the obligations under data protection laws (especially GDPR), you have the **right to file a complaint** at the supervisory authority (It is Úřad pro ochranu osobních údajú - "ÚOOÚ" in the Czech Republic) or another competent supervisory authority of a Member State of the European Union responsible for overseeing compliance obligations imposed by GDPR (in particular, the supervisory authority in the Member State of your usual residence, place of employment or the place where the alleged infringement occurred).
A list of data protection authorities is available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.
You may contact us with requests, complaints or questions regarding these rights as set forth in the "Who we are and how you can contact us?" section above.
Similarly, individuals in countries outside of the EEA and Switzerland may exercise their rights under any applicable data protection laws by contacting us in accordance with the "Who we are and how you can contact us?" section above.

There is no automated decision-making in NTT EU GDC, i.e. a decision based solely on automated processing (including profiling) that would have legal effects for you or would otherwise affect you in a similarly significant way.

vii. You also have the **right to object** to the processing of your personal data if the personal data is processed:

- for the purpose of carrying out a task carried out in the public interest or in the exercise of public authority;
- for the legitimate interests of the controller or a third party; or
- for direct marketing purposes, which includes profiling to tailor the offer to your needs and improve the service we provide.

In the event that you object, we will not process your personal data until we have established serious reasons for processing that outweigh your interests or rights and freedoms, or to determine, exercise and / or defend our legal claims.

If you object to direct marketing processing, we will no longer process your personal data for that purpose.

If any of the above rights are exercised, we will inform you in writing without undue delay of the manner of processing your request.

NTT Europe GDC s.r.o.