Privacy Notice for Team Members and Applicants

Last Updated: April 2024

Introduction

This Privacy Notice ("Notice") is being provided to you by NBG Pay S.A. ("NBG Pay") which is referred to in this Notice as the "Company" and is the data controller of your personal data as defined under the current legislation on the protection of personal data, with special attention to **(i)** Regulation (EU) 2016/679 of the European Parliament and of the Council 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 and; **(ii)** Law 4624/2019 ("Personal Data Protection Authority, measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data that implements into national law Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 and other provisions"), (collectively referred to as the "GDPR").

"Personal data" means any data that relates to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The Company recognizes its responsibilities in relation to the collection, holding, processing, use, disclosure and disposal of the personal data it collects from its team members and job applicants under applicable privacy and data protection laws. The Company takes steps to ensure that your personal data is collected and used for lawful and relevant business purposes. The Company also takes reasonable steps to ensure it maintains appropriate security controls for personal data.

This Notice describes the categories of personal data we may process, how your personal data may be processed, the purposes for which we process your personal data and how we protect your personal data when we collect, process and store it. This Notice does not form part of your contract of employment or engagement. This Notice addresses the use of personal data of prospective, current, and former team members, including temporary workers.

If you have any questions about this Notice or would like to access the information it contains in a different format, please contact your local HR Office.

If you have any questions regarding the processing of your personal data or if you have any concerns about the processing of your personal data, please contact the Data Protection Officer ("DPO"), Compliance Office or HR Office at the following email privacy@nbgpay.com.

What Data do We Process

We may collect various types of personal data about you for the purposes described in this Notice including:

- **Personal details:** your title, name, gender, nationality, civil/marital status, date of birth, age, personal contact details (e.g., address, telephone or mobile number, email), national ID number, passport information, citizenship, immigration and eligibility to work information, driving license, languages spoken, next of kin/dependent/emergency contact information, details of any disability and any reasonable adjustments required as a result;

- **Recruitment and selection data:** skills and experience, qualifications, references, CV and application, interview and assessment data, vetting and verification information, right to work verification, information related to the outcome of your application, details of any offer made to you;

- **Data related to your engagement:** contract of employment or engagement, work contact details (e.g., corporate address, telephone number, email), team member or payroll number, photograph, work location default hours, default language, time zone and currency for location, your worker ID and various system IDs and passwords, your work biography, your assigned business unit or group, your reporting line, your team member/contingent worker type, your hire/contract begin and end dates, terms and conditions of engagement, your cost centre, onboarding and equipment fulfilment information, your job title and job description, your working hours and patterns, whether you are full or part time; your termination/contract end date; the reason for termination; your last day of work; exit interviews, references to be provided to prospective employers, status (active/inactive/terminated); position title; the reason for any change in job and date of change;

- **Regulatory data:** records of your registration with any applicable regulatory authority, your regulated status and any regulatory certificates and references;

- **Remuneration and benefits data:** your remuneration information (including salary/hourly plan/contract pay/fees information as applicable, allowances, overtime, bonus and commission plans), payments for leave/absence (e.g., holiday pay, sick pay, family leave pay), bank account details, grade, national insurance number, PPS, tax information, third party benefit recipient information (e.g., expression of wish and dependents information), details of any benefits you receive or are eligible for, benefit coverage start date, expense claims and payments, loans, deductions, attachment of earnings, salary sacrifice arrangements, childcare vouchers, pension plan information, share scheme participation information and agreements;

- **Leave data:** attendance records, absence records (including dates and categories of leave/time off requests and approvals), holiday dates, requests and approvals and information related to family leave or other special or statutory leave;

- **Absence management data:** absence history, fit notes, details of incapacity, details of work impact and adjustments, details of treatment and prognosis, manager and HR communications, return to work interviews, meeting records, medical reports, occupational health reports, maternity related documentation;

- **Flexible working procedure data:** requests, consideration, correspondence, meeting notes and outcome records;
- **Restructure and redundancy records**: change plans, organisation charts, consultation records, selection and redeployment data;
- **Performance management data:** colleague and manager feedback; your appraisals and performance review information, outcomes and objectives; talent programme assessments and records; succession plans; formal and informal performance management process records; creating, deploying and analysing team member surveys and other feedback;
- **Training and development data:** data relating to training and development needs, or training received or assessments completed;
- **Driving records and related information (as applicable)**: driver license and insurance information; vehicle information including registration number, ownership status, and condition of vehicle, driving record;
- **Disciplinary and grievance data:** allegations, complaints, investigation and proceeding records and outcomes;
- **Health and safety data:** health and safety audits, health and safety screening requests and results (including any health or safety screening implemented in response to a public health emergency or other exigent circumstances), risk assessments, incident reports;
- **Monitoring data (to the extent permitted by applicable laws):** closed circuit television footage, system and building login and access records, download and print records, call or meeting recordings, data caught by IT security programmes and filters, geolocation or other location-based tracking, substance testing data (for specified roles);
- **Team member claims, complaints and disclosures information:** subject matter of employment or contract-based litigation and complaints, pre-claim conciliation, communications, settlement discussions, claim proceeding records, team member involvement in incident reporting and disclosures;
- **Equality and diversity data:** where permitted by law and provided voluntarily, data regarding gender, age, race, nationality, disability status, religious belief and sexuality (stored anonymously for equal opportunities monitoring purposes); and
- Any other personal data which you choose to disclose to us during the course of your engagement whether verbally or in written form (for example in work emails).

Certain additional information may be collected where this is necessary and permitted by local applicable laws.

Special Categories of Personal Data Including Those Relating to Criminal Convictions and Offences

To the extent permitted by applicable laws the Company may collect and process a limited amount of personal data falling into special categories, sometimes called "sensitive personal data". This term means information relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Physical or mental health (including details of accommodations or adjustments);
- Trade union membership;
- sex life or sexual orientation;
- Biometric and genetic data; and
- Criminal records and information regarding criminal convictions, offences or proceedings.

How Does the Company Collect Personal Data

The Company collects and records your personal data from a variety of sources, but mainly directly from you. You will usually provide this information directly to your managers or local Human Resources contact or enter it into our systems (for example, through your self-service access to Workday and payroll vendors such as ADP), your participation in HR processes, emails and instant messages you send or through verbal information which may be recorded electronically or manually. In addition, further information about you will come from your managers or Human Resources or occasionally your colleagues.

We may also obtain some information from third parties: for example, references from a previous employer, medical reports from external professionals, recruitment agencies, information from tax authorities, benefit providers, where we employ a third party to carry out a background check, and from publicly available sources including court records (where permitted by applicable law).

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, CCTV, telephone logs and recordings, instant message logs and email and Internet access logs), if and to the extent permitted by applicable laws. In these circumstances, the data may be collected by the Company or a third-party provider of the relevant service. The collection and use of this type of data is governed by relevant Company policies including the Information Security Policy.

Where we ask you to provide personal data to us on a mandatory basis, we will inform you of this at the time of collection. Failure to provide any mandatory information will mean that we cannot carry out certain HR processes. For example, if you do not provide us with your bank details, we may not be able to pay you. In some rare cases it may mean that we are unable to continue with your employment or engagement as the Company will not have the personal data we believe to be necessary for the effective and efficient administration and management of our relationship with you.

In addition to personal data relating to you, we may ask you to provide the Company with personal data of third parties, notably your dependents and other family members, for purposes of HR administration and management, including the administration of benefits and someone to contact in an emergency. Before you provide such third-party personal data to the Company you must first inform these third parties of any such data which you intend to provide to the Company and of the processing to be carried out by the Company, as detailed in this Notice.

What are the Purposes for which Personal Data is Processed and What is our Legal Basis For Carrying Out the Processing

Your personal data is collected and processed for various business purposes, in accordance with applicable laws and any applicable employment or collective bargaining agreements. We have set out in this Notice the purposes for which we may use your personal data. Personal data may occasionally be used for purposes not obvious to you where the circumstances warrant such use (e.g., in investigations or disciplinary proceedings). We may, where we think it is necessary, provide you with additional information in relevant Company policies to ensure that you understand how your personal data may be used.

The Legal Basis on Which we Process your Personal Data

Whenever the Company processes your personal data, we do so with a legal basis or justification for that processing. In the majority of circumstances, the processing of your personal data will be justified based on one of the following legal justifications:

- The processing is necessary for compliance with a legal obligation to which the Company is subject (for example, disclosing the information to the relevant tax and social security authorities, making statutory payments, avoiding unlawful termination, avoiding unlawful discrimination, meeting statutory record keeping requirements or health and safety obligations); or
- The processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into such a contract (for example collecting bank details to pay your salary or processing information to provide you with the contractual benefits you are entitled to);
- The processing is based on your consent under circumstances for which consent serves as a valid basis for processing (for example, with appropriate consent from you, we will respond to requests for employment verification and employment references in some circumstances, or process other data which you ask us to process for a particular purpose);
- The processing is necessary for the legitimate interests pursued by the Company and such legitimate interests are not overridden by your fundamental rights or freedoms. This includes, for example, the Company's legitimate interest in:
    - Managing its workforce and operating its business. This includes ensuring that team members are properly remunerated, and that this remuneration is set.
    - Managing its workforce and operating its business. This includes ensuring that team members are properly remunerated, and that this remuneration is set at an appropriate level and properly administered; and

Ensuring the effective allocation and organisation of work amongst team members. If you would like further information about the legitimate interests relied upon, and how we have balanced our legitimate interests against your rights and freedoms, please contact your local Data Protection Officer.

The Purposes for Which We use Personal Data

We have identified a number of purposes for collecting and processing your personal data:

Recruitment, pre-employment verification & screening, and offers of employment & onboarding	Considering your suitability to work for us in the role you have applied for, comparing you to other candidates, making recruitment decisions, performing pre-employment screening including credit and background checks.
Future job opportunities	To contact you if you are not successful in your initial application should another potentially suitable vacancy arise during the twelve months following completion of the recruitment process for the role you originally applied for.
Recruitment feedback and complaint	Recruitment documents are kept for a twelve month period post the completion of the recruitment process. This is to assist with any query, challenge or request for feedback received in relation to our recruitment decisions.
Pay and benefits	Providing and administering remuneration, benefits and incentive schemes and making appropriate tax and national insurance deductions and contributions.
Expense reimbursement	Reimbursement of business costs and expenses incurred by team members while performing work on behalf of the Company.
Travel related information	Records related to business travel including air, hotel and vehicle reservation information. Information to assess travel risks to team members as they travel.
Allocating & managing work, identifying & communicating with you, and managing work and job performance	Allocating and managing duties and responsibilities and the business activities to which they relate, including business travel; identifying and effectively communicating with staff including by maintaining staff directories and skill databases; and managing and operating conduct, performance, capability, absence and grievance related reviews, allegations, complaints, investigations and processes and making related management decisions.

Performance and talent management	Managing and operating appraisals or performance reviews and talent programmes.
Training, development and succession planning	Training, development, promotion, career and succession planning and business contingency planning.
Team member relations	Consultations or negotiations with staff or representatives of staff.
Team member engagement	Conducting surveys for benchmarking and identifying improved ways of working and team member relations and engagement at work (these will often be anonymous but may include profiling data such as age to support analysis of results).
Absence and incapacity management	Processing information about absence or medical information regarding physical or mental health or condition in order to: assess eligibility for incapacity or permanent disability related remuneration or benefits; determine fitness for work; facilitate a return to work; make adjustments or accommodations to duties or the workplace; make management decisions regarding employment or engagement or continued employment or engagement or redeployment; and conduct related management processes.
Restructuring and change programmes	Planning, managing and carrying out restructuring or redundancies or other change programmes including appropriate consultation, selection, alternative employment searches and related management decisions.
References	Complying with reference requests where the Company is named by the individual as a referee.
Operating Company Policies & Procedures and Protecting Business Information and Systems	Operating email, IT, internet, social media, HR related and other company policies and procedures. To the extent permitted by applicable laws, the Company carries out monitoring of the Company's IT systems to protect and maintain the integrity of the Company's IT systems and infrastructure; to ensure compliance with

	the Company's IT policies and to locate information through searches where needed for a legitimate business purpose. For information security management purposes, such as the planning and implementation of training and monitoring compliance with Company security policies, procedures, and standards.
Call centre monitoring	Quality and performance monitoring of customer service calls; satisfying the Company's regulatory obligations and maintaining the accuracy and professionalism required for customer service interactions.
Safety, Security and preventing and detecting inappropriate or unlawful activities	Safety and security; satisfying the Company's regulatory or other obligations to supervise the persons employed by it; and preventing, detecting and investigating a wide range of activities and behaviours, whether relating to specific business dealings or to the workplace generally and liaising with regulatory authorities.
Legal compliance	Complying with laws and regulation applicable to the Company (for example maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws, and regulation to which the Company is subject in the conduct of its business).
Ensuring equality of opportunity	Monitoring programmes to ensure equality of opportunity and diversity with regard to personal characteristics protected under applicable anti-discrimination laws.
Commercial transactions or outsourcing	Planning, due diligence and implementation in relation to a commercial transaction or service transfer involving the Company that impacts on your relationship with the Company for example mergers and acquisitions or a transfer of your employment under applicable automatic transfer rules.
Business reporting	For business operational and reporting documentation such as the preparation of annual reports.
Business development and stakeholder management	To operate the relationship with other third parties such as suppliers including disclosure of information to data processors for the provision of services to the Company.

Communication and public relations	Where relevant for publishing appropriate internal or external communications or publicity material including via social media in appropriate circumstances.
HR administration	To support HR administration and management and maintaining and processing general records necessary to manage the employment, worker or other relationship and operate the contract of employment or engagement.
HR record and system management	To manage and maintain HR records, files and systems including technical support and maintenance for HR information systems and managing electronic and hard copy records in line with the Company's HR retention policy.
Litigation	To enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you.
Legal or regulatory disclosures	To comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment), whether within or outside your country.

For further information on the applicable legal bases which we rely on to legitimise these processing purposes, please contact local Human Resources.

The Exemptions we Rely on Where we Process Special Category Personal Data

The special categories of personal data that may be processed by the Company are set out above. Where we process special categories of personal data, it will be justified by a condition set out above and also by one of the following exemptions:

- The processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws;
- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of your working capacity, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, to the extent permitted by applicable laws;

- The processing is necessary to protect your vital interests or of another person where you are physically or legally incapable of giving consent (for example in exceptional emergency situations, such as a medical emergency);
- The processing is necessary for the establishment, exercise or defence of legal claims.
    - Processing is necessary for reasons of substantial public interest, on the basis of applicable law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
    - Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the team member, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in the GDPR;
    - Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of applicable law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; or
    - In exceptional circumstances the processing is carried out subject to your explicit 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 such processing will be provided to you at the time that consent is requested, along with the impact 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 the Company.

The Purposes for Which we use Special Categories of Personal Data

We have identified a number of purposes for collecting and processing your special category personal data:

Your racial or ethnic origin, religion, philosophical or political belief, sexual orientation, gender identity, or disability status	May be used for the collection of statistical data subject to local laws, or where required to record such characteristics to comply with equality and diversity requirements of applicable local legislation or to keep the Company's commitment to equal opportunity under review
Health and medical information	May be used to comply with employment, health and safety or social security laws. For example, to carry out statutory risk assessments and regular health and safety assessments, provide statutory incapacity or maternity benefits, avoid breaching legal duties to you,

	to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to administer the Company's private medical and long term disability schemes, to make reasonable accommodations or adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard. The Company may also process health and medical information to the extent necessary to comply with requirements or recommendations from public health authorities in the context of any public health emergency or similar exigent circumstance.
Where applicable, **details of trade union membership**	May be processed to ensuring that any relevant rights that you may have in connection with any trade union membership are complied with, as required to enable us to meet our obligations under employment law;
Special category personal data of any type	May be used in the management and investigation of any complaint under the Company's grievance, whistleblowing, anti-bullying and harassment or similar policies and procedures or disciplinary procedures where such information is sufficiently relevant to the particular complaint or issue.

Where processing such personal data, we ensure that a relevant exemption applies to allow us to do so. For further information on the applicable exemptions, please contact local Human Resources.

Processing Information Relating to Criminal Convictions and Offences

Personal data relating to criminal convictions and offences will only be processed where authorised by applicable laws. For example:

- A criminal record check may be carried out on recruitment or transfer or intermittently where ongoing screening is required where authorised by applicable laws; or
- An allegation of a criminal offence or conviction arising during your relationship with the Company may be processed where required or authorised by applicable law. For example:
    - Where we have a legal or regulatory requirement to report an offence; or
    - Applicable laws authorise the Company to process information about the offence (e.g., in a disciplinary process) for the purpose of making decisions regarding your relationship with the Company.

For information on the applicable laws we rely on to process personal data relating to criminal convictions and offences, please contact local Human Resources.

Automated Decision Making and Profiling

We may carry out profiling from time to time related to assessment of performance and potential as part of our appraisal process or other career development programs. This is used for development and may be considered for promotion or succession planning but is not used as the sole basis for any decision.

The Company may use profiling technologies, including machine learning, to assist us in maintaining the security of our systems and networks as well as the health and safety of individuals who are present on our premises. We do not rely solely on the output of those tools in making decisions and, where appropriate, we have implemented decision making processes to balance the necessity of such profiling with the fundamental rights of our team members.

We may also encourage participation in activities and programs related to team member benefits, including health and wellness benefits, which include profiling or monitoring technologies to enable the benefit. In these circumstances, team members may be provided with additional information including privacy notice from the benefit provider that gives additional information about how personal data is processed in that context.

Retention of Personal Data

The Company endeavours to ensure that personal data are kept as current as possible and that irrelevant or excessive data are deleted or made anonymous as soon as reasonably practicable. We generally retain personal data for as long as is required to satisfy the purpose for which it was collected. The criteria used to determine our retention periods include:

- The duration of your employment/contract with us and the length of time thereafter during which we may have a legitimate need to reference personal data to address issues that may arise;
- Whether there is a legal obligation to which we are subject, for example, certain laws require us to keep records (such as tax records and pension information) for a certain period of time before we can delete them; and
- Whether retention is advisable in light of our legal position, such as in regard to applicable statutes of limitations, litigation or regulatory investigations.

Further information about our retention periods is available on request, by contacting local Human Resources.

Disclosures of Personal Data

Within the Company, your personal data can be accessed by or may be disclosed internally on a need-to-know basis to:

- Local, regional and global Human Resources, including managers and team members; local, regional and executive management responsible for managing or making decisions in connection with your relationship with the Company or when involved in an HR process concerning your relationship with the Company (including, without limitation, staff from Compliance, Legal, Team member Relations and Information Security);
- System administrators; and

- Where necessary for the performance of specific tasks or system maintenance by staff in the Company teams such as the Finance and IT Department and the Global HR information systems support team.
- Third parties in connection with any proposed or actual reorganization, merger, sale, public offering, joint venture, assignment, transfer or other disposition of all or any portion of our assets or stock (including in connection with any bankruptcy or similar proceedings

Certain basic personal data, such as your name, location, job title, contact information, team member number and any published skills and experience profile may also be accessible to other team members. The security measures in place within the Company to protect your data are set out in the Information Security Policy and Standards.

Your personal data may also be accessed by third parties whom we work together with (including, for example, Workday, ADP and Sum Total, and their associated companies and subcontractors) for providing us with services, such as hosting, supporting and maintaining our HR information systems.

Examples of other third parties with whom your personal data will be shared include tax authorities, regulatory authorities, the Company's insurers, bankers, IT administrators, lawyers, auditors, investors, consultants and other professional advisors, payroll providers, training platform providers, talent management and assessment providers, travel agencies, travel risk vendors, and administrators of the Company's benefits programs. The Company expects such third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security.

Further information about the third parties with whom your personal data is shared is available on request, by contacting local Huma n Resources.

Where these third parties act as a "data processor" (for example a payroll provider) they carry out their tasks on our behalf and upon our instructions for the above-mentioned purposes. In this case your personal data will only be disclosed to these parties to the extent necessary to provide the required services. Where these third parties act as a “data controller” (for example, health benefits providers), we provide personal data to them to the extent required for them to offer their services, including as needed to validate your employment. The third parties who are data controllers may also collect personal data directly from you consistent with the terms and privacy notices they present to you as part of their services.

In addition, we may share personal data with national authorities in order to comply with a legal obligation to which we are subject. This is for example the case in the framework of imminent or pending legal proceedings or a statutory audit.

Security of Personal Data

The Company is committed to protecting the security of the personal data you share with us. The Company uses a variety of technical and organisational methods to secure your personal data in accordance with applicable laws.

We maintain administrative, technical, and physical safeguards designed to protect your personal data against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or

use. Personal data may be stored by the Company, any member of the Global Payments Group and third parties (as described above) physically or electronically, including in a cloud, locally or internationally, and may be accessible by these parties either locally or internationally.

A number of the measures that we use to protect information are set out in our Information Security Policy and Standards.

International Transfer of Personal Data

From time to time your personal data personal data will be transferred to other Global Payments offices in locations outside of your country (which for EU data subjects means outside of the EU) to process for the purposes described in this Notice. This will be applicable for example where a manager from a Global Payments location outside of your country is responsible for reviewing or approving the relevant data or the data is part of a global directory where other individuals need to have access.

Personal data may also be transferred to third parties (e.g., service providers or regulators as set out above), who may have systems or suppliers located outside the EU.

As a result, your personal data may be transferred to countries or territories that do not have the same level of data protection laws that apply in your country. For instance, your personal data may be transferred within the United States where Global Payments corporate offices are located or to any of the affiliates or subsidiaries in the Global Payments Group.

The Company will ensure that appropriate or suitable safeguards are in place to protect your personal data and that transfer of your personal data is in compliance with applicable data protection laws. Your Legal Department or DPO can provide you with additional detail about:

- The countries to which your personal data is transferred; and
- The transfer mechanism on which the Company relies for each of these transfers, including a copy of the mechanism where applicable.

Your Rights as a Data Subject

You have a number of data subject rights, including the 'Right to object', as set out below. There are limits to many of these rights.

Right to Access, Correct and Delete your Personal Data

The Company aims to ensure that personal data it maintains about you is correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to the Company so that we can ensure that your data is up to date.

You have the right to obtain confirmation as to whether or not your personal data are being processed and, where this is the case, to request access to personal data the Company may hold. You also have the right to request correction of any inaccurate data relating to you. You furthermore have the right to request deletion of any irrelevant data we hold about you.

You can see and update some of this data yourself via the relevant HR systems, including Workday and ADP. However, to correct/update other information, you will need to contact local Human Resources.

Data Portability

Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means, you have the right to receive all such personal data which you have provided to the Company 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 Restriction of Processing:

You have the right to restrict our processing of your personal data where:

- You contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy;
- Where the processing is unlawful, but you do not want us to erase the data;
- Where we no longer need the personal data for the purposes of the processing, but you require it for the establishment, exercise or defence of legal claims; or
- Where you have objected to processing justified on legitimate interest grounds (see below) pending verification as to whether the Company has compelling legitimate grounds to continue processing.

Where personal data is subjected to restriction in this way, we will only process it with your consent or for the establishment, exercise or defence of legal claims.

Right to Withdraw Consent

Where we have relied on your (explicit) consent to process particular information and you have provided us with your consent to process data, you have the right to withdraw such consent at any time. You can do this by (i) in some cases deleting the relevant data from the relevant HR system (although note that in this case it may remain in backups and linked systems until it is deleted in accordance with our data retention policy) or (ii) contacting your local Human Resources contact. It will only however be rarely that we rely on your consent to process personal data for your employment or engagement.

Right to Object to Processing Justified on Legitimate Interest Grounds

Where we are relying upon legitimate interest to process data, then you have the right to object to that processing. If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence 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 Complain

You also have the right to lodge a complaint with a supervisory authority if you consider that the processing of your personal data infringes applicable law. This can be the data protection authority in the EU Member

State of your habitual residence, place of work, or of an alleged infringement of the GDPR. In Greece, the relevant supervisory authority is the Hellenic Data Protection Authority (HDPA), www.dpa.gr .

If we do not take action on a data subject request, you have the right to lodge a complaint with a supervisory authority or to seek a judicial remedy.

Notice of Changes

The Company may change or update this Team member Privacy Notice at any time. The “Last Updated” legend at the top of this Notice indicates when this Notice was last revised.

Should we change our approach to data protection, you will be informed of these changes or made aware that we have updated the Team member Privacy Notice so that you know which information we process and how we use this information.