

Who are we?

We are OVIK Health, LLC of 920 Milliken Road, Spartanburg, South Carolina 29303 U.S.A. (“OVIK Health”)

This Privacy Notice explains how we use the personal data that we hold on our current and former employees, agents, consultants, contractors, temporary workers and job applicants.

We may use your information jointly with our affiliated operating companies worldwide. We’ll be the “controllers” of the information you provide to us and will provide you full details on where your personal data is located as explained further below.

What does this Privacy Notice cover?

We at the Company take your personal data seriously. This notice:

- sets out the types of personal data that we collect about you;
- explains how and why we collect and use your personal data;
- explains how long we keep your personal data for;
- explains when, why and with who we will share your personal data;
- sets out the legal basis we have for using your personal data;
- explains the effect of refusing to provide the personal data requested;
- explains where we store your personal data (and whether we transfer your data outside of the European Economic Area, if relevant);
- explains the different rights and choices you have when it comes to your personal data; and
- explains how you can contact us.

What personal data do we collect about you?

Over the course of your relationship with us, it is routine for us to collect, process and store personal information about you. The provision of Personal Data is a requirement necessary to enter into a contract with OVIK Health (as applicable) or a requirement by law or regulation for OVIK Health to administer your employment relationship. The Personal Data processed is limited to the data necessary for carrying out the purpose for which such Personal Data is collected.

Examples of Personal Data processed includes the following:

- Employee data (such as name & initials, age, address, birth certificate number, passport and/or visa, personal and family details, nationality, marital status, next of

kin, photographs, employment and education details/history, financial/payroll details, leisure and interests);

- Contact information (such as phone number, email address, cellular number, emergency contact information)
- Bank account information (such as bank name, account number);
- Organizational information (such as date of hire, job title, occupation, skills, department, disciplinary actions, employee leave information, termination date);
- Salary information (such as bank account number, tax details, chronological compensation data);
- Travel information (such as credit card numbers, expiration date, service code, ID card, passport and visa details, driving license details of employees and some spouses/significant others, travel itineraries, hotel reservation information, expense data);
- Information pertaining to legal obligations (such as employee work permit, health benefits and allowances, social security number, taxpayer identification number);
- Communications information (such as network log-in details, user account ID and computer system usage);
- Location information (such as access controls and CCTV images) and travel locations;

OVIK Health will not collect Personal Data if such collection is prohibited under the applicable data protection laws.

Sensitive Personal Data will be processed in the employment context.

Sensitive Personal Data is defined differently under local privacy law. It can include information such as, racial or ethnic origin, criminal convictions, medical and health information (including for the purposes of obtaining occupational health advice), trade union membership and personal location tracking.

Such Sensitive Personal Data will be processed where specific express consent is obtained, or if one of the particular exemptions provided for by law applies, including:

(a) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of OVIK Health or of the Data Subject in the field of employment and social security and social protection law;

(b) Processing is necessary to protect the vital interests of the Data Subject;

€ Processing relates to Personal Data which is manifestly made public by the Data Subject;

(d) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

€ Processing is necessary for the purposes of preventive or occupational medicine, for the assessment or the working capacity of the employee, medical diagnosis, the provision of

health or social care or treatment or the management of health or social care systems and services.

Where do we collect personal data about you from?

We may collect personal data about you from the following sources:

- Directly from you. This is information you provide to us.
- From an agent/third party acting on your behalf, e.g. from a recruitment or employment agency;
- Through publicly available sources, such as Facebook, Twitter, YouTube and LinkedIn;
- From our Occupational Health Providers;
- By a reference or word of mouth. For example, you may be recommended by a friend or a present or former colleague. Or we may receive a formal written reference from a previous employer or educational establishment;
- From the use of our CCTV cameras. Where we have cameras on our premises, your image and movements may be recorded; and
- From a background check agency.

How and why do we use your personal data?

We process your personal data so that stakeholders like managers, the finance team, and human resources can perform their everyday functions and administer your employment. For example:

- Administer employment (e.g., staffing, global workforce and organizational planning/management, budget planning and administration, education and training, emergency contact, security, providing leased cards, safety, problem resolution, auditing, payment processing, employee communications, payroll, compensation, benefits, expense reimbursement, booking employee business travel);
- Security and access control (e.g., security access badge) and access logs;
- Compliance with legal obligations and legal processes (e.g. audits and processing legal claims);
- Administer employment applicant process (e.g., recruiting employee applicants, communicating with applicant, processing application);
- Compliance with legal obligations regarding employee applicant process (regarding prospective employee application-related information);
- Recruitment, promotion, training, redeployment, and/or career development;
- Administration and payment of wages and other compensation;
- Calculation and administration of all employment related benefits including pensions and national employment services or social security systems;
- Performance review, succession planning and talent management;
- Complying with health and safety regulations, or security measures, e.g. understanding who is at work at any given time;
- Communicating with our associates;
- Organizing events and employee gifts;
- Obtaining outplacement support;
- Obtaining legal and tax advice;
- Responding to audits by third parties and/or governmental authorities;
- Legal processes including court orders; and
- Responding to requests for mortgage and or rental applications
- Managing holiday, sick leave and any other absences (be that family leave, sabbatical or otherwise);
- Carrying out equal opportunities monitoring;
- Processing for vetting and verification purposes to determine your suitability for a particular role;
- Performance management and appraisal, including development via training;
- Dealing with disciplinary matters and any grievance raised by or involving you;
- Ensuring compliance with our rules and processes, for example we may monitor CCTV records and use of our IT systems, including email, internet and intranet, company

mobile and landline phones, computers and tablets to gather evidence in respect of any allegations of wrongdoing.

If there are any circumstances where we feel we need to process data and it is not consistent with these reasons, we will provide you with an updated notification (or seek your express consent where necessary)

How long do we keep your personal data?

How long we keep your information will depend on the purpose for which we use it.

We only keep your information for as long as is reasonably necessary for the purposes set out in this Privacy Notice or, if longer, as required by applicable law or regulation. What this means in practice will vary as between different types of information, and when we consider our approach we take into account any ongoing need for the information as well as our legal obligations, for example in relation to tax, health and safety, employment rights and potential or actual disputes or investigations.

Who do we share your personal data with?

From time to time your personal data may be shared with third parties such our professional advisers, service providers, group companies, and corporate transactional (mergers and acquisitions) partners and advisors for the following purposes.

- Professional advisers: including accountancy and legal firms where they require that information in order to provide the Company with advice;
- Service providers: including those organisations who administer benefits and payroll for Company staff, provide and support our management and data storage systems, and agencies who carry out pre-employment vetting and checks on our behalf;
- Merger partners: it may be that the Company merges or is acquired by a separate organisation, in which case it will become necessary to share personal data with them.

All of these third parties are bound to comply with similar and equally stringent undertakings of privacy and confidentiality.

What legal basis do we have for using your personal data?

Purpose of processing	Legal Basis
Administer Employment (e.g., payment processing, employee communications, payroll, compensation, benefits, expense reimbursement, booking employee business travel)	Contract, Legal Obligation
Administer Employment (e.g., staffing, global workforce and organizational planning/management, budget planning and administration, education and training, emergency contact, security, business travel, provide leased cars, safety, expense reimbursement, problem resolution, auditing, employee communications)	Legitimate Interests
Administer Employment & Compliance with Legal Obligations	Consent
Administer Employment (e.g., emergency contact, security)	Vital Interests
Administer occupation health services	Consent
Compliance with Legal Obligations (e.g., audits and legal claims)	Legal Obligation

Administer Employment Applicant Process (e.g., recruiting employee applicants, communicating with applicant, processing application)	Legitimate Interests
Communications information	Legitimate Interests
Compliance with Legal Obligations Regarding Employee Applicant Process (regarding prospective employee application-related information)	Legal Obligation
Security – Video Surveillance System	Legitimate Interests, Legal Obligation
Security – Access Control System	Legitimate Interests, Legal Obligation
Security – Emergency Mass Notification System	Legitimate Interests
Security – Travel Risk Management System	Legitimate Interests, Opt-in

We process your information:

- As this is necessary for the performance of our employment contract with you or to take steps at your request prior to entering into this contract;
- To comply with our legal obligations including in relation to health and safety at work, monitoring equality and diversity, paying employees and making the necessary deductions for income tax and social welfare contributions like National Insurance;
- As this is necessary in pursuit of our legitimate interests including recruitment and succession planning, organisation and distribution of work, management forecasting, and maintaining an efficient employee benefits program. While there are some risks inherent in any processing personal of personal data, on balance we have considered the risk to your rights of data protection and determined it is outweighed by the significant benefits in maintaining a well-managed and orderly workforce and business. You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on legitimate interests. More information on this right and on how to exercise it is set out below.
- On the basis of your consent for us to process your personal data for a particular purpose, although consent is not something we commonly seek to collect from active employees.

Where we hold sensitive personal data about you (e.g. information relating to your racial or ethnic origin, health etc.) we will only process this data where you have given us, as required by law, your explicit consent or otherwise where this is necessary:

- For the purposes of carrying out the obligations and exercising specific rights of the Company or yourself related to employment and social security and social protection law or a collective agreement;
- To protect your vital interests or the vital interests of another person, if you or they are incapable of providing consent;
- For the establishment, exercise or defence of legal claims; or
- For the purposes of preventative or occupational medicine and for the assessment of your working capacity.

If there are any circumstances where we feel we need to process data and it is not consistent with these reasons, we will provide you with an updated notification (or seek your express consent where necessary).

What happens if you do not provide us with the information we request or ask that we stop processing your information?

We have statutory and contractual obligations under our contract with you and under various employment related legislation that require us to process your information.

If you do not provide the personal data necessary, we may not be able to fulfil our contract with you / perform our obligations under the contract with you (e.g. paying you or providing a benefit), or we may be prevented from complying with our legal obligations (e.g. ensuring the health and safety of our workers)

Do we make solely automated decisions concerning you?

No, we do not carry out solely automated decision making or automated profiling.

Where do we store your personal data? Do we transfer your personal data outside the EEA?

If we or our service providers transfer personal data outside of the country where the Company is based or, where relevant, outside of the EEA, we will always require that appropriate safeguards are in place to protect the information that is transferred. For example, a portion of our centralised Human Resources, Compliance, and Payroll functions are performed outside of the EEA, in the USA, so we have put in place safeguards to protect personal data processed in or accessed from the USA. You can obtain a copy of the

safeguards in place for such transfers by contacting us using the details at the end of this Privacy Notice.

How do we keep your personal data secure?

We ensure the security of your personal data by implementing a specific set of technical and organisational security measures that are based on controls published by the Center for Internet Security (CIS Critical Controls). These controls call for the use of encryption, firewalls, and other measures that ensure we provide a level of security appropriate to the risk presented by a particular situation.

We also take steps to ensure all our subsidiaries, agents, affiliates and suppliers employ adequate levels of security.

What rights do you have in relation to the personal data we hold on you?

You have a number of legal rights when it comes to your personal data, and we describe them here. Further information about your rights can be obtained from the data protection regulator in your country.

Rights	What does this mean?
1. The right to be informed	You have the right to be provided with clear, transparent and easily understandable information about how we use your information and your rights. This is why we're providing you with the information in this Privacy Notice.
2. The right to lodge a complaint	You have the right to lodge a complaint about the way we handle or process your personal data with your national data protection regulator.
3. The right of access	You have the right to obtain access to your information if we're processing it, and certain other information similar to what provided in this Privacy Notice. This is so you're aware and can check that we're using your information in accordance with data protection law.
4. The right to rectification	You are entitled to have your information corrected if it's inaccurate or incomplete.
5. The right to erasure	This is also known as 'the right to be forgotten' and, in simple terms, enables you to request the deletion or removal of your information where there's no

Rights	What does this mean?
	compelling reason for us to keep using it. This is no absolute right to erasure; there are exceptions.
6. The right to restrict processing	You have rights to 'block' or suppress further use of your information. When processing is restricted, we can still store your information, but may not use it further. We keep lists of people who have asked for further use of their information to be 'blocked' to make sure the restriction is respected in future.
7. The right to data portability	You have rights to obtain and reuse your personal data for your own purposes across different services.
8. The right to object to processing	You have the right to object to certain types of processing, including processing based on our legitimate interests and processing for direct marketing.
9. The right to withdraw consent	If you have given your consent to something we do with your personal data, you have the right to withdraw your consent at any time. Doing so does not affect the validity of the processing we performed prior to when you withdrew your consent.

How can you make a request to exercise your rights?

To exercise any of the rights above, or to ask a question, contact us using the details set out at the end of this Privacy Notice.

How will we handle a request to exercise your rights?

We'll respond as soon as we can, generally within one month from when we receive your request. If we expect your request is going to take us longer to fulfil, we'll come back to you within that first month and let you know.

We usually act on requests and provide information free of charge, but we may charge a reasonable fee to cover our administrative costs of providing the information for baseless or excessive/repeated requests and requests for further copies of the same information. Alternatively, the law may allow us to refuse to act on such requests.

How can you contact us?

If you have questions on the processing of your personal data, would like to exercise any of your rights, or are unhappy with how we've handled your information, please contact us

here: We are OVIK Health, LLC of 920 Milliken Road, Spartanburg, South Carolina 29303 U.S.A., Privacy@milliken.com

If you're not satisfied with our response to any complaint or believe our processing of your information does not comply with data protection law, you can also make a complaint to the data protection regulator in your country.

Our Data Protection Manager can also be reached at Privacy@milliken.com