

Employee Privacy Notice

DATA PROTECTION AND DISCLOSURE OF INFORMATION

Data controller details

This Privacy Notice applies to the data processing activities of Scopemarkets Services CY Limited and its affiliated entities ("Scopemarkets" the "Company"). For the purposes of this Privacy Notice, "Affiliated Entity" means a company which, is from time to time, a subsidiary or a holding company or a subsidiary of a holding company of Scopemarkets.

Scopemarkets is the data controller for the processing of your personal data.

Any reference to 'us', 'our', 'we' in this Privacy Notice is a reference to Scope Markets. Similarly, any reference to 'you', 'your', 'yours' or 'yourself' in this Privacy Notice is a reference to current or former employees, contractors as the context requires unless otherwise stated.

Scopemarkets, is the data controller for the processing of your personal data in relation to those services.

We are aware of our obligations under the General Data Protection Regulation (GDPR) and we are committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR, the types of data that we hold on you as an employee, ex-employee or contractor of the Company. It also sets out how we use that information, how long we keep it for and other relevant information about your personal data and details your rights in respect of our processing of your personal data.

Types of data we process

Depending on the circumstances and applicable laws, we may collect the information listed below to enable us to employ you (please note that this list is not exhaustive and may be updated from time to time):

- your personal details including your name, address, date and place of birth, nationality, citizenship
- Contact details, email address, phone numbers
- your photograph
- copy of passport or national identity card
- gender
- marital status, dependents, emergency contact details and their contact numbers
- medical or health information including whether or not you have a disability for the purpose of arranging health insurance benefits and covering sick leave days
- information used for equal opportunities and fair treatment monitoring about your religion or belief and ethnic origin information included on your CV including references, education history and employment history, information that your referees provide us about you, information that our existing employees may tell us about you, or information provided by third party sources such as job sites
- copies of diploma's and certificates
- documentation relating to your right to work in the Republic of Cyprus
- bank details
- tax number, social insurance number
- current and previous job titles, job descriptions, salary and other payment details, pension entitlement, hours of work and other terms and conditions relating to your employment with us
- letters of consent, formal warnings and other documentation with regard to any disciplinary proceedings
- internal performance information including measurements against targets, formal warnings and related documentation with regards to capability procedures, appraisal forms
- leave records and documentation including annual leave, family leave, sickness absence etc.
- details of your criminal record and if required details of your bankruptcy records.
- training details
- CCTV footage
- building entry card records, company equipment records and other acknowledgement forms
- signed agreements and other contractual documentation

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms and submit documents at the start of your employment or contract and during your employment, for example, your bank and emergency contact details, where appropriate. Other details may be collected directly from you in the form of official documentation such as your passport, utility bill or other evidence.

In some cases, we will collect data about you from third parties, such as your referees, employment agencies, former employers, when gathering references or credit reference agencies.

Personal data is kept in personnel files or within the Company's HR and IT systems.

Why we process your data

We process and/or might process personal information of yours as per the provisions of GDPR:

- in order to perform the employment contract or contract for services that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- in order to protect your vital interests
- where something is done in the public interest and;
- where you have given consent for one or more specific purposes.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to carry out the employment contract that we have entered into with you and ensure you are paid.

We also need to collect your data to ensure we are complying with legal requirements such as ensuring any tax or other obligations are met, carrying out checks in relation to your right to work in the Republic of Cyprus and making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the Company. We have set these out below:

- making decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc.
- making decisions about salary and other benefits
- providing contractual benefits to you
- maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake relevant measures if the need arises
- offering a method of recourse for you against decisions made about you via grievance procedures
- assessing training needs
- implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- gaining expert medical opinion when making decisions about your fitness for work
- managing statutory leave and pay systems such as maternity leave and pay etc.
- business planning and restructuring exercises
- dealing with legal claims made against us
- preventing fraud
- ensuring our administrative and IT systems are secure and robust against unauthorised access
- better understand and define working behaviour, expectations and processes from employees and its expectations for future job specifications, evaluate employees' performances, improve employees' training and identify new areas requiring training and performance monitoring

We reserve the right to monitor the use of our premises, software, equipment, and similar resources and assets. In occasions such monitoring occurs, it may result in collecting some of your personal information. This monitoring may concern the CCTV cameras use in and around our premises.

Special categories of data

Special categories of data are data relating to your health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, trade union membership, genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly we will process special categories of data when;

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data for the purposes of equal opportunities monitoring, in our sickness absence management procedures, to determine reasonable adjustments and arranging health insurance benefits.

We do not need your consent if we use special categories of personal data in order to carry out our obligations or exercise specific rights in the field of employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Criminal conviction data

We shall collect criminal conviction data where the law permits us. This data will usually be collected at the recruitment stage, however, may also be collected during your employment or other contract, if required to perform the services.

We may process this data under of our regulatory obligations to undertake appropriate due diligence checks on all staff.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your employment or other agreement. If you do not provide us with the data needed to do this, we will be unable to perform those duties e.g. ensuring you are paid correctly.

We may also be prevented from confirming, or continuing with, your employment with us or extend your probation period, if you do not provide us with this information e.g. confirming your right to work in the Republic of Cyprus.

Sharing your data

Your data will be shared with colleagues within Scopemarkets where it is necessary for them to undertake their duties. This includes, for example, your line manager for their management of you, and payroll for administering payment under your employment agreement.

We will never sell, trade, or rent your personal data to others however; we may share your information with selected third parties including:

- Internally within Scopemarkets on a “need to know” basis, including with members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with the vacancy and IT staff;
- Business partners, auditors, contractors, advisers, affiliates and service providers of Scopemarkets (Insurance companies, banks credit score agencies, background check agencies etc.). Scopemarkets will generally require those third parties to keep your personal data confidential and secure. Third parties are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions;
- Other third parties if we choose to sell, transfer, or merge parts of our business, or our assets or we may seek to acquire other businesses or merge with them;
- Credit reference agencies or a verification company to conduct checks on you to verify the information you have provided

- We may share information with regulators, law enforcement agencies, information protection authorities, and other relevant competent authorities, governmental or judicial bodies, as well as with other competent third parties, as may be required if the Company believes that you performed any act or omission that the Company believes to be violating any applicable law, rules, or regulations, or if the Company is required, or believes that it is required by law to share or disclose your information to applicable authorities or to any other third party.
- Anyone else authorized by you.

Third party service providers such as credit referencing agencies or verification agencies may keep a record of any searches performed on our behalf and may use the search details to assist other companies in performing their searches.

Transfers of personal data outside the EEA

During the processing of your personal data, certain personal data may be transferred to entities situated or operating in territories outside of the European Economic Area, including any territory which does not offer a level of protection for the rights and freedoms of data subjects which is equivalent to the data protection standards afforded within the European Economic Area. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with the GDPR or other relevant laws.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss, disclosure, destruction and or abuse. We have implemented appropriate technical and organizational measures and processes to guard against such breaches. Such measures and safeguards may include encryption during information transmission and storage, strong authentication mechanisms and the segmentation of digital architecture to zones that are policed and protected. We have implemented a strategy of 'least possible access' and periodically review existing access. While such systems and procedures significantly reduce the risk of security breaches and the inappropriate use of personal information, they do not provide absolute security. The Company will regularly review its security posture with reference to the latest standards to effectively eliminate the likelihood of any form of misuse.

Where we share your data with third parties as per the present policy, we provide written instructions to them to ensure that your data are held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, which will be the duration of your employment (on in the case of contractors the duration of the contract) with us and after termination of your employment or contract, we will retain your information for the least period required in order to fulfill our legal or regulatory obligations and for our legitimate business purposes.

We may retain personal information for longer periods than required by law if it is in our legitimate business interests as far as the law does not restrict us from doing so and unless you wish to exercise any of your rights (as described further below) and such exercise does not contradict the Company's legal obligations, or if it is impossible for us to delete them for technical reasons. We may also keep information for research or statistical purposes. If we do so, we will make sure that your privacy is always protected and only use it for those purposes. Where we hold your data in relation to communications with clients, this will be held under our regulatory obligations.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- **the right to be informed.** This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- **the right of access.** You have the right to access the data that we hold on you. To do so, you should make a subject access request to the Company.
- **the right for any inaccuracies to be corrected.** If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- **the right to have information deleted.** If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- **the right to restrict the processing** of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct

- **the right to portability.** You may transfer the data that we hold on you for your own purposes
- **the right to object to the inclusion of any information.** You have the right to object to the way we use your data where we are using it for our legitimate interests
- **the right to regulate any automated decision-making and profiling** of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to store and use the data where so permitted by having a legitimate reason for doing so or where required by law, regulation or by any other competent authorities.

If you wish to exercise any of the rights explained above, please contact us using the contact details below.

Contact Us

If you have any queries regarding privacy issues or the content of this privacy notice, you can email us on HR@scopemarkets.com, write to us at: Scope Markets HR, Scope Markets, 19, Spyrou Kyprianou Ave, Silver House, Ground Floor 3070, Limassol, Cyprus or call us + 35725262578.

What if you have a complaint?

If you have a concern about any aspect of our privacy practices, you can make a complaint. This will be acted upon promptly. To make a complaint, please contact us via one of the methods set above. If you are not satisfied with our response to your complaint, you have the right to lodge a complaint with our supervisory authority, Commissioner for the Protection of Personal Data in Cyprus (the "Commissioner"). You can find details about how to do this on the Commissioner's website at http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page1i_gr/page1i_gr?opendocument.

Amendments to this policy

The Company may change and update the terms of this Privacy Policy from time to time and will notify all employees accordingly.

Governing law and jurisdiction

In respect of issues not addressed in the present Privacy Policy, the law of Cyprus will apply and the competent courts for the settlement of any possible dispute shall be the Cypriot Courts.