Job Applicant Privacy Notice

Table of Contents

Introduction

Crido Taxand R. Namysłowski i Wspólnicy sp.k. and Crido group companies (hereinafter referred to as „Crido") set great store by the protection of the confidentiality and privacy of the data we collect. One of our key responsibilities is to ensure appropriate security and legitimate use of personal data. We take the security of job applicants' personal data with utmost seriousness.

This Job Applicant Privacy Notice (the "Notice") serves as the basis for the processing of your personal data by Crido. Crido processes personal data for a number of purposes. Each purpose may entail a different method of data collection, different lawful basis for data processing, data use, disclosure and storage.

Your data is controlled by the Crido company to which you submitted your job application documents (e.g., CV, covering letter). All Crido group companies however have signed an agreement on joint personal data control. Under the agreement, each and every Crido group company can lawfully process your personal data within the scope set forth in this Notice.

Scope of this Notice

As with most companies, we store and process a wide range of information, some of which concerns Crido job applicants.

This Notice concerns persons who seek employment with Crido, for example, as an employee, partner, independent contractor, etc. All reference to employment is taken to mean work in the broad sense of the word, whether performed by an employee, contractor, consultant or partner.

Wherever the word "you" or its equivalent is used, reference is to any person to whom this Policy is directed.

Categories of data subject to processing

"Personal data" is a term defined in the 2018 Data Protection Act and means any information relating to an identified or identifiable natural person, covering not only facts about that natural person but also that person's intentions and any opinions about that person.

"Processing" means any operation which is performed on personal data such as collection, recording, disclosure and erasure.

"Sensitive personal data" and **"special categories of data"** is data consisting of information about the racial or ethnic origin, political opinions, religious or philosophical beliefs, a natural person's health, sexual orientation or their sex life, trade union membership, as well as genetic data and biometric data, and is subject to special protection under separate provisions of the 2018 Data Protection Act.

The categories of personal data we process differ depending on your position and terms and conditions of your employment or engagement (where applicable). Generally, Crido processes personal data for the purpose of its own business activity, including for the purpose of providing services to its clients, for the purpose of management, administration, recruitment and for legal and regulatory reasons. Typically, personal data categories comprise the following information:

- **Your personal data** – for example, first name and surname, date of birth, place of birth, sex, private contact details, contact details of persons to reach out to in the event of emergency / closest relatives, citizenship, knowledge of foreign languages, etc.

- **Information gathered during the recruitment / selection process** – for example, personal data in your CV, job application form, notes taken during your job interview, your references, candidate vetting records.

Sources of personal data

Some of your personal data processed by Crido is data you have shared with us yourself in the course of applying for a job at Crido. Such data includes, for example, your contact details, the address you reside at (your correspondence address), the degree to which you were educated and your employment record to-date, as well as data about your status under immigration law, and the possibility of taking up lawful employment in a given country.

Note that we may obtain data from external recruitment officers, employment agencies and other organisations in the course of the recruitment process.

Disclosure of personal data

Your personal data may be viewed internally by your supervisors, partners, HR staff, and, in some circumstances, by your colleagues. We may also transfer your data outside the organization, for example, to third parties with whom you maintain relations or to payroll processing companies.

Internal disclosure: Your personal data may be disclosed to your superiors, project partners, HR staff and data controllers for the purpose of employment, data control and data management, as described above in this Policy.

Your data will also be shared with other Crido group companies where this is required for the company's administrative purposes, in particular, for access to asset-sharing arrangements or our central HR database, as well as for group reporting purposes.

Disclosure to third parties

We will disclose your personal data to persons outside Crido only if the disclosure is consistent with the basis for data processing in our Policy, does not breach any provisions of the law, and is fair to you; in particular, if the disclosure does not infringe your rights and freedoms.

We may disclose your personal data if doing so is necessary to protect our legitimate interests or the legitimate interests of the third parties (but we will refrain from disclosing it if our interests are subordinate to your interests and rights, in particular, your right to privacy). We may also disclose your data if you consent to our doing so.

From time to time, your data may also be disclosed to courts, regulatory, government and law enforcement bodies, should this be required by the law. We can reassure you that, whenever we disclose your personal data in such circumstances, every possible precaution is taken in relation to the data recipient and that there is a necessary agreement in place to ensure the integrity and security of the data in accordance with the law.

Special circumstances under which your data may be disclosed include:

- disclosure to organisations and consultants who process data on our behalf and assist us in providing related services or making offers of services, such as payroll processing companies, insurers and other service providers, our bank and external organisations that run our IT systems and manage our data. Our external service providers will be required to follow our instructions and will be subject to contractual restrictions that protect your data
- disclosure to external recipients of electronic communication (such as email messages) that contains your data
- disclosure to regulatory or statutory bodies, as and when needed, and
- disclosure, in strict confidence, to a potential buyer of our business or our company for target evaluation purposes, but only if a sale is being contemplated.

Some third parties to whom we may disclose your personal data are themselves independent data controllers. These include: health insurance providers, travel services providers (including tour operators), legal advisors and accountancy firms. This means that they take their own decisions regarding data processing, and that you are advised to become familiar with their privacy protection measures and the rules which govern their use of your personal data.

Retention of data

Our general rule is that we store personal data only as long as it is needed to fulfill the purpose for which we have collected such data, or you have supplied it to us, or for a similar purpose. We will keep your personal data for the period of your employment and for a certain time thereafter.

In some cases, we are bound by legal and regulatory requirements to keep certain information for a set period of time, including after your employment or engaement has been terminated.

In certain other cases, we keep information intentionally in order to be able to deal with enquiries or resolve disputes which we believe may subsequently arise.

The personal data of job applicants (other than that of a successful applicant) will as a rule be erased upon the completion of the recruitment process or once the consent has been withdrawn by persons who have consented to their data being processed for the purpose of future recruitment.

Cross-border data transfer

The global nature of some of the Crido entities' operations within the international Taxand network (the "Network") means that your personal data may be transferred to other entities from the Network or to external providers or partners that are based outside the European Economic Area, including (but not limited to) our members in Africa, the Middle East, in the Asia-Pacific region and the United States, that is, to countries that do not guarantee a level of privacy protection equivalent to that in the European Union. Transfer of data to other Network members will in each case be based on the adequacy rule (data minimization) and purpose limitation, in accordance with the relevant provisions of the GDPR and the opinions and instructions of the working party set up under Art 29.

In the event of transfer of your personal data outside the EEA by third parties, we will take appropriate steps to ensure that your personal data is adequately protected, for example, by obtaining assurances that the third parties have the relevant certificates compliant with the data protection certification programmes.

Legal rights of the data subject

You have the right to exercise control over your personal data, which includes the right of access to your data, demand for its removal and the right to register your objection to the way your data is managed. These rights are subject to certain exclusions which we can apply, while other rights (such as the right to demand that data be erased) apply only in limited circumstances. For more information on your rights, see Enclosure 2 to this policy.

Policy status

The Policy is not part of your agreement with Crido which is the basis for your employment, your provision of services or contract work.

Enclosure 1

The purpose and lawful basis for the processing of data by Crido

Pursuant to the 2018 Data Protection Act, there are a number of justified and lawful bases for the processing of your data by Crido. Sometimes more than one basis is applicable. We have grouped these bases into dedicated categories: Agreement, Legal Requirement, Legitimate Interest, and Consent. They will aid you in a better understanding of each basis type.

Term	Basis for processing	Explanation
Agreement	Processing is necessary to perform the agreement we have signed with you or to take the steps you have asked us to take before the agreement is signed.	Refers to the discharge of our contractual obligations and exercise of our contractual rights.
Legal Requirement	Processing is necessary for compliance with a legal requirement.	Processing ensures we can comply with legal and regulatory requirements, e.g., ensuring a safe working environment and non-discrimination or compliance with regulatory requirements.
Legitimate Interest	Processing is necessary to pursue our or a third party's legitimate interests.	We or a third party have legitimate interests that we pursue in carrying on our business activity, managing and administering it, and in the processing of your data in relation to such interests. Your data will not be processed on this basis if our or a third

		party's interests are subordinate to your interests, your rights and your freedoms.
Consent	You have given explicit and informed consent to your personal data being processed.	The general rule is that the processing of your data in relation to your employment (including the processing of sensitive personal data) does not require your consent. There may be instances where we have to undertake some actions, such as giving references, using your image, etc. These will require your consent.

Whenever we process your sensitive personal data or need to ensure that one of the bases for processing referred to above applies, we will check first if at least one of the conditions for the processing of sensitive personal data is met. Here is a simplified list of conditions for processing:

- processing is necessary for the discharge of your or our contractual obligations and exercise of your employment rights, where this is permitted by law or under a collective agreement
- processing of your data which you have made public yourself (e.g., if you tell your friends that you are ill)
- processing is necessary for the establishment, exercise or defence of legal claims
- processing is necessary for the provision of health care or treatment, medical diagnosis and for assessing the working capacity of the employee
- subsequent processing, rarely used for the purpose of employment, to which you have given prior explicit consent.

The Policy sets out the purposes for which we process your personal data. More detailed information, including examples of personal data and the bases for their processing, have been presented in the table below.

The examples in the table are not a closed list. Note too that not all examples of data processing apply to every Crido group company or to every employee, and that your individual case will depend on the type of agreement you have signed.

Purpose of processing	Examples of personal data subject to processing	Valid lawful bases for personal data processing
Recruitment, evaluation of job applications or offer of employment, recruitment decision making and applicant vetting before employment	Any information relating to your job application and our evaluation, your references, any steps we can take to verify the information you have supplied or to vet your candidacy, as well as any information regarding your employment rights. If necessary, we may have to process information about your health, disability and workstation adaptation.	▪ Contract ▪ Legitimate interests ▪ Where necessary for compliance with employment law requirements ▪ Consent
Managing your employment agreement, including the signing process, performance and any modifications to it	Information about the current terms of your employment, including remuneration and benefits, such as participation in a pension scheme, life insurance policy and medical insurance, any bonus or employee share schemes	▪ Contract ▪ Legal obligation ▪ Legitimate interests
Keeping of your contact details or contact details of persons we will contact on your behalf, e.g., in the event of an emergency	Your address and telephone number, contact details for emergency situations, information about the closest relatives	▪ Legitimate interests
Payroll management / corporate accounting	Information regarding your bank account, pension scheme contributions, taxes and national insurance	▪ Contract ▪ Legal obligation ▪ Legitimate interests

Making and keeping a record of your absences at work	Information about the hours worked, holiday and other absences, including parental leave and sick leave	▪ Necessary for compliance with employment law requirements ▪ Necessary for assessing your working capacity ▪ Legitimate interests of Crido
Supporting and managing your work and your efficiency	Information related to your work, everything you do at work and your performance results, including the documents you have created and the emails you have written or documents and emails concerning you. Management information concerning you including notes from meetings, and performance evaluation results. Information about your adherence to internal rules. Information about accusations, investigations and lawsuits or complaints in which you are involved or may be involved, directly or indirectly.	▪ Contract ▪ Legitimate interests ▪ Necessary for compliance with employment law requirements
Steps taken concerning employee health, incapacity, and any necessary rectification of your data	Information about your health, your medical reports and medical interest reports We will process the personal data of the employees who have joined a vaccination programme.	▪ Necessary for assessing your working capacity ▪ Necessary for compliance with employment law requirements ▪ Consent
Changes to or termination of your employment	Information on any aspect of current employment that may affect future	▪ Contract ▪ Legitimate interests

	employment prospects or terms of employment, including an offer of promotion, changes to the pay grade or benefits, changes to terms of employment or termination of employement	
Personal security and security of IT systems	Access ID card records and records obtained from other similar cards Records of your use of our IT systems: computers, telephones and other devices, including passwords	▪ Crido's legitimate interests include security and monitoring of our data network and business systems ▪ Crido's legitimate interests include protection of the safety of our colleagues and our resources, crime prevention and detection
Disclosure of information for the purpose of future employment	Your employment record with us	▪ Consent
Sharing of information with third parties in connection with planned transactions	Information about your agreement with us and other information that may be required by third parties, e.g., potential buyer, seller or employer	▪ Legitimate interests

Enclosure 2

Rights of data subjects whose data is collected and data security breach notification procedure

The following is a summary of your fundamental rights under the provisions of the 2018 Data Protection Act in the event of breach of your data security:

Right to access your data

You have the right to obtain from us information about whether we process your personal data. If we do process your data, you have the right to know:

- why we process your data (purpose of processing)
- what group of data we process
- what data recipients or categories of data recipients we have disclosed your data to (or may disclose your data to) – this concerns, in particular, recipients in countries other than countries being members of the European Economic Area or international organisations
- how long we are planning to process your data (if this is possible to determine) and by reference to what criteria we have determined this period

Right to obtain a copy

You have the right to obtain from us a copy of the personal data we process. We will supply you with a copy free of charge.

Right to rectify data

You have the right to ask that we rectify incorrect personal data without delay or complete any incomplete data. We have seven days to comply.

Right to erasure (right to be forgotten)

You have the right to ask for your personal data to be erased if:

- your personal data is no longer necessary in relation to the purpose for which we have collected it
- you have lodged an effective objection or withdrawn consent to the processing of your data (and there are no legitimate grounds for further processing)
- your data has been processed unlawfully

Right to restrict processing

You have the right to ask that the processing of your data be restricted.

In some cases, even if you have asked us to restrict the processing of your personal data, we will continue to process the data where this is lawful, or in accordance with the advice and instructions of a regulatory body.

Right to data portability

Everyone has the right to transfer their data to another IT environment. To do so, you must ask us to transfer the data, which we will do by encrypted email.

If we cannot separate your data from other data which is kept in our systems, we may put your request on hold until we can jointly agree on which data can be transferred.

Right to object to processing

You have the right to object to the processing of your personal data in certain circumstances. Each time this happens, you must tell us what it is you specifically object to.

Data security breach notification procedure

A data security breach occurs where the data controller accidentally or unlawfully destroys, loses, modifies, discloses or shares your personal data.

Should a data security breach take place at Crido, we will notify:

- a supervisory authority (if we have assessed the likelihood of personal rights or freedoms having been infringed to be higher than low), and
- you (if we have assessed as high the risk of infringement of your personal rights and freedoms).

We will report any personal data security breaches without delay – if possible, **within 72 hours** of the discovery of the data breach. Our data security breach notification will include advice on how to limit any adverse effect of the breach. If we deem the risk of infringement of personal rights and freedoms to be high, we will notify directly the persons who have been affected. Should personal notification involve disproportionate effort, we will make a public communication instead.