

Employees' Privacy Policy of Clerides, Anastassiou, Neophytou LLC

(the "Policy")

At **Clerides, Anastassiou, Neophytou LLC (the "Firm")**, we care about the privacy and security of your personal information and we take measures to ensure that your personal information is properly handled while in our possession, as well as in the possession of others to whom we may disclose them.

This Policy mainly explains when and why we collect our employees' personal information or the personal information of those who apply for employment to our Firm, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this Policy from time to time.

In compliance with the EU General Data Protection Regulation (the "GDPR"), our Firm has appointed a Data Protection Officer (the "DPO"). In case you have any questions with regards to this Policy or any question or complain with regards to how your personal data is handled, you can contact our DPO as follows:

Name: Dr. Christiana Markou

Email: dpo@cyplaw.com

Tel.: +357 22377863

Fax: +357 22377860

Address: 2, Amfipoleos street, Marcou Tower Office 201, 2025 Strovolos, Nicosia.

This Policy was last updated in 25th May 2018.

Who are we?

Clerides, Anastassiou, Neophytou LLC (HE 224964)

Address: 6 Kolokotroni, 3040, Limassol Cyprus

Tel: +357 25 274050

Fax: +357 25 370704

Email: info@cyplaw.com

Website: <http://www.cyplaw.com/Welcome.html>,

How do we collect information from you?

We obtain information about you:

- when you apply to be hired to our Firm during the recruitment process by submitting your application and/or resume directly or indirectly via the employment agency you are associated with;
- through the form you fill in and submit along with the relevant attachments provided that you are hired;
- during your employment through your work performance and exercise of duties, for the payment of your salary and/or other benefits, as well as relevant communications or notes and;
- by submitting and/or justifying requests to us regarding any licenses, changes to your terms of service or any other requests you might have.

What type of information is collected from you?

The personal information we collect may include your name, date of birth, passport or identity card number, ARC number, social security number, telephone number, your address, email address, your IBAN number, copies of your passport or identity card, your employee number, your employment department, your occupation or job title, your license to practice, the date of your employment to our company, your salary, bonuses, participation in a healthcare plan, details of your expenses for the performance of your work (such as transport costs, telephones, customer care costs etc.), your employment contract/letter and your work assignments, your confidentiality agreement, your signature when you sign your contract/letter of employment or any other document in the scope of your duties, your

arrival and departure time from your work facilities, your access card/code to these facilities, your leaves and your requests for a leave, the parts of our systems that you have access and in some cases the actions you take on these systems, your billable hours, the communications you have with customers, partners or other third parties via emails, warning letters and correspondence, the event and reason for any dismissal or non-recruitment, reports and/or evaluations of your performance, as well as any other information you voluntarily provide through your employment application, such as your resume, employment letters, referral letters, academic and other qualifications, certificates/diplomas for attending seminars required by the CBA or otherwise and your current pursuit study.

Finally, we collect sensitive data, in particular health data, in the form of medical certificates, or otherwise, upon submitting for a sick leave or a maternity leave. Also, in cases where there may be an accident at work, data on accident conditions and health implications are collected.

How is your information used?

We use your information lawfully in accordance with: (i) **Article 6(a) of the GDPR** i.e. for purposes you have consented to; (ii) **Article 6(b) of the GDPR** i.e. as necessary to conclude or perform a contract with you; (iii) **Article 6(c) of the GDPR** i.e. to comply with obligations imposed by law (such as tax and anti-money laundering legislation) and (iv) **Article 6(f) of the GDPR**, i.e., as necessary for legitimate interests we pursue as a business and (v) **Articles 9(2)(a) and 9(2)(b) of the GDPR** relating to sensitive data, specifically health data, which are processed with your explicit consent, or for the purposes of complying with labor and/or social security legislation respectively.

We provide more details immediately below to help you understand how exactly we use your information:

Article 6(b) of GDPR

- In order to examine your job application, we will conduct the relevant procedure by assessing your suitability for the position and to enter into an employment contract with you and inform you of your recruitment or rejection of application, as well as for purposes of implementing the employment contract such as for the payment of salaries and/or other benefits and the examination of leave requests.

Article 6(c) of GDPR

- In order to comply with our obligations arising from employment and tax legislation, including social security legislation and the GDPR, amongst others by sending you relevant circulars, updates and information.

Article 6 (1)(f) of GDPR

- to inform you of any changes to our Firm's policies or employees' privacy policy;
- to communicate with you in the context of our relationship for the purposes of the better organization of business and efficient administration of our company;
- for the protection and safety of our facilities and our property;
- for better customer service and to facilitate resolution of disputes that may arise between customer or claimant and employee;
- possibly to perform staff surveys and statistics, after we first anonymize the relevant personal data;

Article 6 (a) of GDPR

- to send you communications you have requested, such as a response to a query or complaint;
- any other purpose for which we have obtained your prior consent.

Article 9(2)(a) and (b) of GDPR

- to manage or respond to your sick leave requests, or your participation in a health insurance plan.
- grant you access to our premises through the card control system

In case you need further explanation on how we use your information, you are welcome to contact the DPO whose info are mentioned at the beginning of this Policy.

Where and how long do we retain your information for?

Your information is mainly stored in physical files and computer servers in our premises.

We retain your data for as long as our employment relationship lasts, as well as for a period after it is terminated as required for the purposes of our compliance with tax and labor laws, as well as to be able to defend or to bring any legal action against or on behalf of our Firm. In general, we maintain your information as long as we maintain a contractual relationship with you and up to six (6) years after the termination or conclusion of that relationship.

In the event that we have received your consent to the collection or use of information for a particular purpose, we will maintain this information until that purpose is achieved while it is relevant or until you withdraw your consent or oppose the processing thereof.

In case we do not conclude to an employment relationship with you, we retain your data for a period of up to one (1) year from the date you submitted your application/resume for employment to our Firm.

Emails exchanged between members of the Firm that do not relate to any of the Firm`s clients and/or prospective and/or potential clients and/or the business and/or prospective and/or potential of the Firm or an affiliate of the Firm and/or affairs of the Firm or an affiliate of the Firm and which emails relate exclusively and directly to the employment relationship between you and the Firm, are maintained for as long as the contractual relationship between us lasts and up to six (6) years after expiration and/or termination of the contractual relationship and/or the termination of any disputes and/or claims that may be pending or ongoing.

In the event that another maximum retention period is set by the Data Protection Commissioner applicable to employee data, we will maintain such a fixed maximum retention period.

After the aforementioned retention periods, we will withdraw the above information from our systems by deleting this information or by keeping them completely anonymous so that you can no longer be identified through them. In the latter case, we will not delete all information, but only data such as the name, address, email address which reveal that this information belongs to you.

Who may have access to your information?

We will not sell or rent your information to third parties and we will not share it with third parties for marketing purposes.

We may pass your information to third party service providers. Such third parties may be technical service providers providing us with the software systems or technical facilities (or their maintenance) necessary to conduct administrative tasks inherent in the provision of managing our employees, their salaries and leaves. We only disclose to them the personal information that is absolutely necessary to deliver the service or perform the said task and when required by the regulation, we have a contract in place that requires them to keep your information secure and in accordance with the principles and rules of the GDPR and not to use it for their own direct marketing purposes or for any purposes other than to provide the service or complete the task as explained above.

Please note that we do **not** monitor your emails, and this is done automatically by using your e-mail service. Only partners, managers and supervisors have access to inward emails sent from third parties and exercise this possibility for supervision purposes, when necessary and in case an employee leaves the company, to secure the information that may be on that account.

We may also pass your information to our lawyers, accountants/auditors or other parties to the extent necessary to defend or institute legal claims and to comply with legal obligations with regards to financial accounts and tax reasons respectively.

We may also transfer personal information to our banks in Cyprus, specifically for paying your salaries or other payments or benefits. Banks are controllers of personal data themselves and are bound by all of the obligations of the GDPR and must have their own privacy policies which you should consult.

We may transfer your personal information to a third party as part of a sale of some or all of our business and assets or sale of any ownership interest in our Firm to any third party or as part of any business restructuring or reorganization in which case we will take measures to ensure that all data protection principles and related rights as derived by the GDPR are fully complied with during all stages of the relevant transfer.

Finally, we may disclose your information to public, tax, judicial, regulatory or supervisory authorities or other authorities, if disclosure is required by law or other arrangement or an order is issued by a court of law or as part of compliance with our licensing conditions imposed by such authorities.

What are your rights?

You may at any time send us any of the following requests and we will meet them the earliest possible and in any case, within 1 (one) month from the date of receipt of your request and inform you about the action we have taken. If your request is for any reason complex to examine or meet, we will ask you for an extension before the aforementioned one-month period expire.

If we have legitimate reasons to refuse to satisfy your request, we will inform you accordingly and in this case, you have the right to submit a relevant complaint to the Cyprus data protection authority, namely, the Data Protection Commissioner, <http://www.dataprotection.gov.cy/> if you believe that our decision is unjustified.

These are the requests you can submit to us:

A request that we permanently delete all or some of your information from our records (*right to be forgotten or to erasure*), for example when we no longer have reasons to retain it.

A request for you to access your information that we keep in our records (*right of access*).

A request that we provide you with a copy of your information that exists in our records, in digital or hard copy form. If you require more than one copy, we may charge you a maximum of EUR 100,00 as administrative cost (*right to a copy*).

A request that we update or correct your information that we keep in our records (*right to rectification*), for example, in case it is outdated or contains errors or inaccuracies.

A request that we provide you with information of yours we keep in our records in a structured, commonly used and machine-readable format or forward it in such form to another provider of your choice, if such forwarding or transfer is technically possible (*right to portability*). *Please note that this right applies only in relation to data that you yourself have provided to us with and which we process by electronic means in the context of a contract between you and our company or because you have consented to us doing so.*

A request that we stop doing anything with your information without however deleting it from our records (*right to restriction of processing*). In this case, we will restrict access to your data.

A request that we stop processing your information on the basis of legitimate interests pursued by our Firm as explained under the fourth question of this Policy or in the name of the public interest (*right to object*). If we receive any such request, we will stop processing your data for the said purposes unless we have compelling reasons to refuse to do so and we will inform you accordingly.

If you wish to exercise any of the above rights you will be able to do so by contacting our DPO at any of the contact details stated above in this Policy, preferably by email, specifying the type of right you seek to exercise.

Please note that before acting upon any of your above requests, we may require you to prove your identity, if we are in doubt about your true or correct identity. If we cannot identify you, i.e., we do not hold personal data belonging to the person you are saying you are, we will inform you accordingly and we will not act upon your request.

What security measures do we apply to protect your information?

When you give us personal information, we take organizational and technical measures to ensure to keep it secure and protected against unauthorized disclosure, alteration, accidental loss or other violation.

Transferring your information outside the European Union

We do not transfer your information to a country that is not a Member State of the EU.