Privacy Statement

This Privacy Statement is issued by LCK Financial Services Ltd ("LCK", "we" or "us"), a limited liability company incorporated in Cyprus.

LCK is dedicated to protecting the confidentiality and privacy of information entrusted to us in accordance with the EU General Data Protection Regulation (GDPR) and National Law L.125(I)/2018. Please read this Privacy Statement to learn about your rights, what information we collect, how we use and protect it.

1. Who are we?

This Privacy Statement applies to LCK Financial Services Ltd.

2. How do we collect personal data?

- Directly – We obtain personal data directly from individuals in a variety of ways, including obtaining personal data from individuals who provide us with their business card(s), complete our online forms, subscribe to our newsletters and preference centre, register for seminars, webinars, attend meetings or events we host, visit our offices or for recruitment purposes. We may also obtain personal data directly when, for example, we are establishing a business relationship, performing professional services through a contract, or through our hosted software applications.
- Indirectly – We obtain personal data indirectly about individuals from a variety of sources, including recruitment services and our clients:
    - Public sources – Personal data may be obtained from public registers (such as Companies Registrar), news articles, sanctions lists and crime prevention agencies and internet searches.
    - Social and professional networking sites – If you register or login to our websites using social media (e.g., LinkedIn, Facebook, or X) to authenticate your identity and connect your social media login information with us, we will collect information or content needed for the registration or login that you permitted your social media provider to share with us. That information may include your name and email address and depending on your privacy settings, additional details about you, so please review the privacy controls on the applicable service to set how much information you want shared with us.
    - Business clients – Our business clients may engage us to perform professional services which involve sharing personal data they control as part of that engagement. For example, we will review payroll data as part of an audit, and we often need to use personal data to provide global mobility services. Our services may also include processing personal data under our clients' control on our hosted software applications, which may be governed by different privacy terms, policies and notices.

- Recruitment services – We may obtain personal data about candidates from an employment agency, and other parties including former employers or academic references.

3. What categories of personal data do we collect?

We may obtain the following categories of personal data about individuals through direct interactions with us, or from information provided through client engagements, from applicants, our service providers and through other situations including those described in this Privacy Statement.

- Personal data – Here is a list of personal data we commonly collect to conduct our business activities:
  - Contact details (e.g., name, company name, job title, work and mobile telephone numbers, work and personal email and postal address).
  - Professional details (e.g., job and career history, educational background and professional memberships, published articles)
  - Family and beneficiary details for insurance and pension planning services (e.g., names and dates of birth).
  - Financial information (e.g., taxes, payroll, investment interests, pensions, assets, bank details, insolvency records).
  - CCTV at our sites may collect images of visitors.
- Special categories of personal data – We typically do not collect special categories of personal data about individuals other than our own employees. In some circumstances it is necessary for LCK to process special categories of personal data of our employees and other third parties. Other than where such personal data is made public by the individual themselves, such processing would only be undertaken as necessary for LCK to exercise its rights and obligations as an employer (including for occupational health purposes), protect the vital interests of individuals, establish or defend legal claims or with the explicit consent of the individual(s) concerned. Examples of special categories of personal data we may obtain, or otherwise hold, include:
  - Personal identification documents that may reveal race, religion or ethnic origin, possibly biometric data of private individuals, beneficial owners of corporate entities, or applicants.
  - Expense receipts submitted for individual tax or accounting advice that reveal affiliations with trade unions or political opinions.
  - Adverse information about potential or existing clients and applicants that may reveal criminal convictions or offences information.
  - Information provided to us by our clients in the course of a professional engagement.
  - Diversity and equal opportunity information volunteered by participants in certain LCK professional empowerment programmes.
  - Health data where the processing is necessary to assess, monitor and control spread of infectious diseases and to provide a safe environment for our employees, clients and suppliers.

- Child data – Our sites are not intentionally designed for or directed at children under the age of 14. It is our policy never to knowingly collect or maintain information about anyone under the age of 14, except as part of an engagement to provide professional services. Although we do not intentionally collect information from individuals under 14 years of age, we may occasionally receive details about children attending performances and other events we host with their parents or guardians (e.g., gala, work party/gathering).
- Location-based data – We may process geographical locations you enter when seeking an office near you.

4. What lawful reasons do we have for processing personal data?

We may rely on the following lawful reasons when we collect and use personal data to operate our business and provide our products and services:

- Contract – We may process personal data to perform our contractual obligations owed to (or to enter into a contract with) the relevant individuals.
- Consent – We may rely on your freely given consent at the time you provided your personal data to us.
- Legitimate interests – We may rely on legitimate interests based on our evaluation that the processing is fair, reasonable and balanced. These may include:
    - Delivering services to our clients – To deliver the professional services our clients have engaged us to provide including information on new products and services.
    - Direct marketing – To conduct and analyse our marketing activities. To deliver timely market insights and speciality knowledge including tailor-made online experience we believe is welcomed by our business clients, subscribers and individuals who have interacted with us.
    - Monitor our IT systems – Prevent fraud or criminal activity and protect our IT systems.
    - Corporate responsibility – Comply with our corporate and corporate social responsibility commitments.
- Legal obligations – We may process personal data to meet our legal and regulatory obligations or mandates.
- Public Interest – We may process personal data to perform a specific task in the public interest or in the exercise of official authority vested in us.
- Vital Interests – We may process personal data to protect the vital interests of the individual or another natural person.

5. Why do we need personal data?

We aspire to be transparent when we collect and use personal data and tell you why we need it, which typically includes:

- Providing professional advice and delivering reports related to our tax, advisory, audit and assurance, mergers and acquisitions and other professional services. Our services may

include reviewing client files for quality assurance purposes, which may involve processing personal data for the relevant client.

- Promoting our professional services, products and capabilities to existing and prospective business clients.
- Sending invitations and providing access to guests attending our events, seminars and webinars or our sponsored events.
- Personalising online landing pages and communications we think would be of interest based on interactions with us.
- Administering, maintaining and ensuring the security of our information systems, applications and websites.
- Authenticating registered users to certain areas of our sites.
- Seeking qualified candidates, and forwarding candidate career inquiries to our HR team, which may be governed by different privacy terms and policies.
- Processing online requests, including responding to communications from individuals or requests for proposals and quotations.
- Contacting journalists regarding company press releases, invitations to annual press parties, highlighting messages that may be of interest on specific industry topics.
- Helping support clients to run a series of development programs for education and learning purposes to inform leaders in the healthcare, civil service and other industries.
- Complying with legal and regulatory obligations relating to anti-money laundering, terrorist financing, fraud and other forms of financial crime.
- Compiling health and safety data (directly or indirectly) following an incident or accident. Indirect data can take many forms including an incident report, first aider report, witness statements and CCTV footage.
- Collecting health data to assess, monitor and control spread of infectious diseases and to provide a safe environment for our employees, clients and suppliers.

6. Do we share personal data with third parties?

We may occasionally share personal data with trusted third parties to help us deliver efficient and quality services. These recipients are contractually bound to safeguard the data we entrust to them. We may engage with several or all the following categories of recipients:

- Parties that support us as we provide our services (e.g., providers of telecommunication systems, mailroom support, IT system support, archiving services, document production services and cloud-based software services).
- Professional advisers, including lawyers, auditors and insurers.
- A potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of our business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it.
- Parties that support as with anti-money laundering, client conflicts and independence checks.

- LCK may disclose personal data in order to respond to requests of courts, law enforcement or other government and regulatory agencies (e.g., CyPAOB, ICPAC, MOKAS) or to other third parties as required by, and in accordance with, applicable law or regulation.
- Health government bodies and external service providers (health, facilities, estate management) to assess, monitor and control the spread of infectious diseases.
- Payment, marketing and recruitment services providers.

LCK will not transfer the personal information you provide to any third parties for their own direct marketing use.

7. Do we transfer your personal data outside the European Economic Area (EEA)?

We store personal data on servers located in the European Economic Area (EEA). We may transfer personal data to reputable third-party organisations situated inside or outside the EEA when we have a business reason to engage these organisations. Each organisation is required to safeguard personal data in accordance with our contractual obligations and data protection legislation.

8. Do we use cookies?

Our websites may use cookies. Where cookies are used, a statement will be sent to your browser explaining the use of cookies.

9. What are your data protection rights?

- Access – You can ask us to verify whether we are processing personal data about you, and if so, to provide more specific information.
- Correction – You can ask us to correct our records if you believe they contain incorrect or incomplete information about you.
- Erasure – You can ask us to erase (delete) your personal data after you withdraw your consent to processing or when we no longer need it for the purpose it was originally collected.
- Processing restrictions – You can ask us to temporarily restrict our processing of your personal data if you contest the accuracy of your personal data, prefer to restrict its use rather than having us erase it, or need us to preserve it for you to establish, exercise, or defend a legal claim. A temporary restriction may apply while verifying whether we have overriding legitimate grounds to process it. You can ask us to inform you before we lift that temporary processing restriction.
- Data portability – In some circumstances, where you have provided personal data to us, you can ask us to transmit that personal data (in a structured, commonly used, and machine-readable format) directly to another company if is technically feasible.

- Automated Individual Decision-making – You can ask us to review any decisions made about you which we made solely based on automated processing, including profiling, that produced legal effects concerning you or similarly significantly affected you.
- Right to Object to Direct Marketing including Profiling – You can object to our use of your personal data for direct marketing purposes, including profiling. We may need to keep some minimal information to comply with your request to cease marketing to you.
- Right to Withdraw Consent – You can withdraw your consent that you have previously given to one or more specified purposes to process your personal data. This will not affect the lawfulness of any processing carried out before you withdraw your consent. It may mean we are not able to provide certain products or services to you and we will advise you if this is the case.
- If you would like to exercise your Data Subject Rights, you can email info@lckfs.com. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information or to exercise any of your other rights. This helps us to ensure that personal data is not disclosed to any person who has no right to receive it. No fee is required to make a request unless your request is clearly unfounded or excessive. Depending on the circumstances, we may be unable to comply with your request based on other lawful grounds.

10. What about personal data security?

We have put appropriate technical and organisational security policies and procedures in place to protect personal data (including sensitive personal data) from loss, misuse, alteration or destruction. We aim to ensure that access to your personal data is limited only to those who need to access it. Those individuals who have access to the data are required to maintain the confidentiality of such information. We may apply pseudonymisation, de-identification and anonymisation techniques in efforts to further protect personal data.

If you have access to parts of our websites or use our services, you remain responsible for keeping your user ID and password confidential. Please be aware that the transmission of data via the Internet is not completely secure. Whilst we do our best to try to protect the security of your personal data, we cannot ensure or guarantee the security of your data transmitted to our site; any transmission is at your own risk.

11. How long do we retain personal data?

We retain personal data to provide our services, stay in contact with you and to comply with applicable laws, regulations and professional obligations that we are subject to. Unless a different time frame applies because of business need or specific legal, regulatory or contractual requirements, where we retain personal data in accordance with these purposes, we retain such personal data for seven years.

12. Do we link to other websites?

Our websites may contain links to other sites, including sites that are not governed by this Privacy Statement. Please review the destination websites' privacy notices before submitting personal data on those sites. Whilst we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content, security, or privacy practices employed by other sites.

13. Who can you contact for privacy questions or concerns?

If you have questions or comments about this Privacy Statement or how we handle personal data, please direct your correspondence to: LCK, 62 Athinas Street, Athina Court, Office 105, 8010, Paphos, Cyprus or email info@lckfs.com. We aim to respond within 30 days from the date we receive privacy-related communications.

If you are not satisfied with the response you receive, you may also contact the Cyprus Data Commissioner's Office at

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/6AE8EE38D05E28C6C22581FD004202B2 to report concerns you may have about LCK in Cyprus.

Data Commissioner's website: https://www.dataprotection.gov.cy

14. Do we change this Privacy Statement?

We regularly review this Privacy Statement and will post any updates to it on this webpage.