finductive

PRIVACY POLICY

For the purposes of this policy, Finductive shall be referred to as the "Data Controller / we / us", and Account Holders, prospective clients or any person sharing their personal information with us shall be referred to as the "Data Subjects".

We at Finductive are Data Controllers of Data Subjects' personal data and shall process Data Subjects personal data, whether alone or in conjunction with others, as specified below, for the purpose of engaging business (regardless of the extent or the outcome of such engagement), subject to the conditions of business and any resulting contractual relationship, and for the other reasons set out in this Policy.

Regarding the processing of information and for the remit of this present Policy, as part of our operational procedures, the following personal data is usually processed by us, as follows:

a. first and last name/s of the contact person(s);

b. (correspondence) address data; phone number/s;

c. e-mail address;

d. Skype ID;

e. due diligence data and information;

f. academic or educational or other professional data, as applicable;

g. financial information, as applicable.

Such data and information may relate to information provided via the Website, certifications, contractual agreement/s (whether public documents or private agreements), correspondence, substantiating documentation that may be either directly or indirectly related to the verification of the information and the personal data (whereby use of third party commercial databases may be used) and to such contractual agreement/s, associations, products, services and markets Data Subjects or the entity Data Subjects are representing may be involved in regularly or on an occasional basis.

In individual cases, we also process personal data that we may obtain from publicly available sources, which may be accessible both online and/or offline, free of charge or against the payment of a fee, such as registers, phone lists, commercial registers, civil registries, which are legitimately provided and collated.

In the course of conducting our business and obliging with legal, regulatory and contractual duties, we will be processing data obtained from third parties, be they known to you, entities with which Data Subjects do business, entities that formally hold or process data about Data Subjects or otherwise.

Where personal data has been obtained from other Parties (who are not connected to the Group), such as – for example when we are in the process of ascertaining the nature and verification of the documents and information submitted or otherwise made available to us – unless Data Subjects are already aware of such a transfer of data or have already consented to such a transfer, we will be in a position to provide Data Subjects with the following information, as applicable:

a. the identity and the contact details of the Data Controller that provided such personal data and, where applicable, of the controller's representative;

b. the contact details of the Data Protection Officer of such Data Controller, where applicable;

c. the purpose/s of the processing for which the personal data are intended as well as the legal basis for the processing;

d. the categories of personal data concerned;

e. the recipients or categories of recipients of the personal data, if any.

We do not collect personal information on children aged under 16, unless a parent or legal guardian has given his/her consent for this.

1. How And Why We Use Data Subjects Personal Data

As further detailed, the legal basis for us to process personal data may be explained as follows:

a. where there is a Legal Requirement:

- We will use Data Subjects personal data to comply with our obligations at Law:
- to assist any public authority, regulatory, judicial or criminal investigation body;
- to identify Data Subjects when Data Subjects contact us; and
- to verify the accuracy of data we hold about you.

b. consent (where Data Subjects have asked that a third-party share information about Data Subjects with us and the purpose of sharing that information is not related to the performance of a contract or services by us to you, we will process Data Subjects information based on Data Subjects consent). We may use and process Data Subjects personal information where Data Subjects have consented for us to do so for the following purposes of correspondence, that is, to contact Data Subjects via email or via post or otherwise. Data Subjects may withdraw their consent in any of these ways at any time;

c. necessary to engage in business activity and eventually perform a contract or to take steps to enter into a contract;

d. To provide the services which Data Subjects, or an entity with which Data Subjects are employed or are a shareholder, beneficial owner or officer in, request, we shall need to process the Data Subjects personal data in order to be able to give effect to the contract;

e. Our legitimate business interests.

We may use and process Data Subjects personal data where it is necessary for us to pursue our legitimate business interests as a business operation for amongst the following or related purposes:

- conduct and promote business in a streamlined and cost-efficient manner, in line with the best market practices;
- consolidate accounting and operations reporting requirements;
- compliance with legal, regulatory and corporate governance obligations and good practice;
- prevention of fraud and other criminal activities.

f. where a third party has shared information about Data Subjects with us, we will presume that the Data Subjects have consented to the sharing of that information, we will have a legitimate interest in processing the personal data within.

g. where Data Subjects have given their consent to having their Personal Data shared with a third party service provider in order to apply for such third party's services.

h. It may also be the case that third parties may pass on information about Data Subjects to us if Data Subjects have infringed or potentially infringed any of our rights at Law (whereby we may use such information for the possible assertion or exercise of legal claims).

2. Others Who May Receive Or Have Access To Data Subjects Personal Data

This section sets out the circumstances in which we may need to disclose information about Data Subjects to third parties and any additional purposes for which we use Data Subjects information. We require all third parties to respect the security of Data Subjects personal data and to treat it in accordance with the law. Where we are the Data Controller, we do not allow our Data Processors to use Data Subjects personal data for their own purposes and only permit them to process Data Subjects personal data for specified purposes and in accordance with our instructions.

As further detailed here below, access to Data Subjects personal data is restricted to:

a. our employees and representatives;

b. our affiliates;

c. our third-party service providers, agents, delegates, sub-contractors and/or any other party which may be engaged or otherwise used by us) for any purpose in connection with our remit.

Any selected individuals with access to Data Subjects personal data shall be subject to the same duties and limitations under this Policy. We may also disclose Data Subjects data if we are under a duty to disclose or share Data Subjects personal data to comply with any legal obligation, judgment or under an order from a court, tribunal or authority.

3. Our Group Affiliates

We may need to receive and/or transfer Data Subjects personal data to our affiliated companies within the Group. It is within our Legitimate Business Interests to conduct our duties in terms of Legal and Regulatory expectations, promote business efficiency and operational processes within the Group, in line with current best business practices.

4. Our Business Partners, Suppliers And Related Service Providers

Depending on the nature of the activity in question, we may disclose or make available Data Subjects data to certain third-party business partners, service providers, agents, sub-contractors and other organisations for the purposes of providing services to us or directly to Data Subjects on our behalf. Such third parties include administrative services that provide services to us. When we engage third party service providers, we only disclose to them any personal data that is necessary for them to provide their service and ensure that the contract in place requires them to keep personal data secure and not to use it other than in accordance with our specific instructions.

Sharing Data Subjects information with third parties, which are either related to or associated with the running and management of our business and/or relationship with you, where it is necessary for us to do so.

5. Disclosure Of Data Subjects Personal Data For Legal Reasons

In line with our legitimate interest and legal obligations, if we suspect that criminal or potential criminal conduct has or is taking place (including possible identify theft, money laundering, funding of terrorism, fraud), we will in certain circumstances need to contact an appropriate authority, such as the police. This could be the case, for instance, if we suspect that a fraud or a cybercrime has been committed or if we receive threats or malicious communications towards us or third parties. We will generally only need to process Data Subjects personal data for this purpose if Data Subjects were involved, or affected by such an incident, in some way or capacity or there are suspicions thereto. We will also use Data Subjects data in connection with the exercise or potential exercise of our legal rights. We may need to use Data Subjects information if we are involved in a dispute with Data Subjects or a third party e. g. either to resolve the dispute or as part of any mediation, arbitration or court resolution or similar.

6. Public Agencies And Regulatory, Judicial Or Criminal Investigation Bodies

From time to time, we may need to share Data Subjects personal data with regulatory or public authorities as well as judicial or criminal investigation authorities that may have jurisdiction over our entities or business. If false or inaccurate information is provided to us as part of Data Subjects liaising or relationship

with us, and fraud is identified or suspected, details may be passed to fraud prevention agencies, which could include personal data. We will cooperate with all competent authorities and law enforcement and prevention agencies, whether based within the EU/EEA or otherwise.

7. Other Ways We May Share Data Subjects Personal Data

In more seldom cases, we may transfer Data Subjects personal data to a Third Party as part of a sale of some or all of our business and assets or as part of any business restructuring or reorganisation; sharing Data Subjects information with a prospective or actual purchaser or seller in the context of a business or asset sale or acquisition by us, a merger or similar business combination event, whether actual or potential.

Legal basis for processing: legitimate interests of sharing Data Subjects personal data with a prospective purchaser, seller or similar person to facilitate such a transaction to take place.

8. Where We Store Data Subjects Personal Data

Certain personal data may be transferred to countries outside the EU/EEA. This may happen where any of our Group affiliates, servers or those of our third-party service providers are located in a country outside of the EU/EEA.

These countries may or may not have similar Data Protection laws to the EU/EEA. In such cases, we will take steps to ensure that appropriate security measures are taken with the aim of ensuring that Data Subjects privacy rights continue to be protected as outlined in this Policy.

9. Marketing

Subjects to the Data Subject's consent, we will contact Data Subjects by conventional mail or as provided here below about latest information, events and updates and offers related to our operations, as may be applicable, from time to time. We may use telephone, email or any other electronic means to inform Data Subjects about such offers. We may also want to inform Data Subjects about activities or services supplied by any associates, agents and by other carefully selected third parties for which we will also require Data Subjects consent.

Data Subjects may opt out of such marketing services by:

a. by sending an e-mail to info@finductive.com

b. writing to any one of our offices;

c. sending such request to the Finductive Data Protection Officer by e-mail to compliance@finductive.com.

10. Data Retention Policy

If we collect Data Subjects personal data, the length of time we hold Data Subjects personal data depends on several factors, such as:

a. the nature of the information we hold;

b. the purpose for which this is processed;

c. compliance with our legal obligations (such as crime detection and prevention, accounting, social security and taxation reporting laws);

d. industry practices and/or accepted standards;

e. whether Data Subjects and we are in a legal or some other type of dispute with third parties or each other.

We do not retain personal information in an identifiable format for longer than is necessary.

Where possible and on a case by case basis, we minimise, pseudonymize, anonymise and/or destroy personal data, when the purpose/s for which it has been collated has been fulfilled/ duly satisfied.

11. Criteria For Determining Retention Periods

Otherwise than is excepted to in the following section, we retain Data Subjects personal data for no longer than necessary, considering the following:

a. the purpose(s) and use of Data Subjects information both now and in the future (such as whether it is necessary to continue to store that information to continue to perform our obligations under a contract with Data Subjects or to contact Data Subjects in the future);

b. whether we have any legal obligation to continue to process Your data (such as any record-keeping and reporting obligations imposed by relevant law or regulation);

c. whether we have any legal basis to continue to process Your data (such as Data Subjects consent);

d. any relevant agreed industry practices on how long information should be retained;

e. the levels of risk, cost and liability involved with us continuing to hold the information;

f. how hard it is to ensure that the information can be kept up to date and accurate; and

g. any relevant surrounding circumstances (such as the nature and status of our relationship).

12. Specific Retention Periods

Certain statutory obligations may require longer retention periods for certain personal data. Therefore, a single retention period that applies to all personal data which Data Subjects hold across the board may not always apply; different periods should be established, as follows.

a. Website. A website user who no longer accesses the website, all their information obtained for this purpose will be deleted within one (1) calendar year, unless any of the exceptions below apply.

b. Correspondence and enquiries. When Data Subjects make an enquiry or contact us by email or via our contact form, we will retain Data Subjects information for as long as it takes to respond to and resolve Data Subjects enquiry, and for a further six (6) months, after which point, we will delete Data Subjects information.

c. Mailing list and other formal general communications. We retain the information Data Subjects used to sign up for our newsletter for as long as Data Subjects remain subscribed (i.e. Data Subjects do not unsubscribe) or if we decide to cancel our newsletter service, whichever occurs first.

d. Contractual relationship. Your personal data will be retained for the duration of Data Subjects contractual relationship with us and, upon its expiry or termination, for a subsequent period of six (6) calendar years to allow for the possible assertion or defence of claims and litigation, as may arise. At the same time, we may be required to retain certain categories of Data Subjects personal data for a fixed longer period (e.g. transaction data), due to statutory obligations and regulated reporting requirements.

13. Data Subject Rights

Under Data Protection law, and as a Data Subject for the purpose of the GDPR, Data Subjects have several rights regarding to their personal data.

Data Subjects can exercise the rights outlined above by contacting us using any of the channels below:

a. by sending an e-mail to info@finductive.com

b. writing to any one of our offices;

c. sending such request to the Finductive Data Protection Officer by e-mail to compliance@finductive.com.

For as long as we retain Data Subjects personal data, these rights allow Data Subjects to exercise control over the way in which Data Subjects personal information is processed. Data Subjects are entitled to:

d. Access Data Subjects personal data. They may ask us for a copy of the personal information we hold. They can ask us about how we collect, share and use Data Subjects personal information;

e. Update and correcting Data Subjects personal information. If Data Subjects believe that certain personal information, we hold is inaccurate or out of date, Data Subjects can look for the information to be corrected;

f. Withdrawing Data Subjects consent. You can change Data Subjects mind whenever Data Subjects give us consent, such as for direct marketing;

g. Restrict and object. They have the right to restrict or object to the processing of Data Subjects personal information or using automated decision making;

h. Delete Data Subjects information (right to be forgotten). Data Subject may ask us to delete all its personal information;

i. Transferring Data Subjects personal data (right to Portability). Where possible we can share a digital copy of Data Subjects information directly with Data Subjects or another organisation indicated by you.

In relation to the exercising of certain rights, we may ask Data Subjects for personal data to confirm identity and, where applicable, to help us to search for Data Subjects personal information. Save for exceptional cases, where we will provide the necessary information and explanation, we will respond to Data Subjects within ***thirty (30) running days*** after we have received this information or, where not required, after we have received Data Subjects request.

14. Verifying Data Subjects Identity Where Data Subjects Request Access To Their Personal Data

Where Data Subjects request access to Data Subjects personal data, we are required by law to use all reasonable measures to verify Data Subjects identity before doing so. These measures are designed to protect Data Subjects and reduce the risk of identity fraud, identity theft or general unauthorised access to Data Subjects personal data. Where we possess appropriate personal data about Data Subjects on file, we will attempt to verify Data Subjects identity using that personal data. In default, we may require original or certified copies of certain documentation to verify Data Subjects identity before we are able to provide Data Subjects with access.

15. Handling of Data Breaches

In the event of a Personal Data breach, that is, a breach (of security) leading to the accidental, unauthorised and/or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, or any other threatening enforcement proceeding against the Company and/or the Data Processor pertaining to the processing of Personal Data, We will notify the Subject Person about this without undue delay, except and unless:

a. we have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b. we have taken subsequent measures which ensure that the high risk to Data Subjects rights and freedoms is no longer likely to materialise; or

c. it would involve disproportionate effort.

16. Data Subject's Rights of Redress

Without prejudice to any other administrative or judicial remedy, GDPR allows every Data Subject the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual

residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. Thus, if Data Subjects do not agree with the response received from Finductive, Data Subjects are also entitled to lodge a complaint with the Office of the Information and Data Protection Commissioner at the details indicated below. The Data Protection Supervisory Authority responsible is:

Information and Data Protection Commissioner

Floor 2, Airways House, High Street, Sliema, SLM 1549. MALTA.

Telephone (+356) 2328 7100 **Email idpc.info@gov.mt**

17. Security / Links

a. Security Measures We Put In Place To Protect Data Subjects Personal Data

We are committed to implement and maintain appropriate and sufficient technical and organisational security measures to protect Data Subjects personal data against unauthorized, accidental or unlawful destruction or loss, damage, alteration, unauthorized disclosure or access or otherwise processed and shall be solely responsible to implement such measures. We shall ensure that our people are aware of such technical and organizational security measures and we shall ensure that such personnel is bound by a duty to keep Data Subjects personal data confidential. The technical and organisational security measures in this clause shall mean the particular security measures intended to protect Data Subjects personal data in accordance with any privacy and data protection laws.

b. Measures Taken To Secure Data Subjects Data

Finductive and/or its Data Processors shall implement and maintain, at all times, appropriate organisational, operational, managerial, physical and technical measures to protect the Personal Data and any other data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access so that all processing is in compliance with Laws and written instructions, especially where the processing involves the transmission of data over a network. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

Technical safeguards shall include all technical security controls defined or indicated by us, following the recommendations as laid out in ISO/IEC 27000 series (Information Security Management Systems standards or equivalent). Access to Personal Data is restricted to authorised and properly trained personnel with a well-defined “need-to-know” basis, and who are bound by appropriate confidentiality obligations.