DATA PROTECTION POLICY

VERSION 2.0.

INTRODUCTION

1. PURPOSE

The purpose of CHRISTABEL'S CORPORATE SERVICES LTD (hereby referred to as 'we', 'us', 'our' "**CHRISTABEL**", or the 'Company') DATA PROTECTION POLICY is to:

(i) *explain* CHRISTABEL'S data protection obligations and commitments to comply with data protection and laws;

(ii) *describe* CHRISTABEL'S employees' responsibilities and accountability for data protection;

(iii) *provide* information on how to contact CHRISTABEL for requests and enquiries in connection with personal data.

2. LEGAL BACKGROUND

Christabel Corporate Services Limited, efficiently provides corporate and business support services to global clients.
When you contact us via any form of communication for any reason on our website or through email or otherwise we will collect and process the personal data you willingly provide to us when contacting us solely for the purpose of addressing your query.

Data Protection laws govern how CHRISTABEL handles personal data in the countries where we operate.

Those laws define our legal status and obligations. Where CHRISTABEL determines the purpose, means and conditions of processing personal data, we are a decision-maker, generally referred to as a data controller. Where we act as a service provider on behalf of others, we are a data processor.

The European Union (EU) has sought to ensure the protection of personal data rights through legislation. Therefore, the EU has drafted and passed the toughest privacy and security law in the world the General Data Protection Regulation 2016/679 (hereby referred to as '**the GDPR'**) on transferring personal data of EU data subjects both within and outside the European Economic Area (hereby referred to as '**the EEA**'). The GDPR regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.

These laws apply to all transfers of data within the CHRISTABEL group of companies and from CHRISTABEL to other third parties.

CHRISTABEL group of companies consists of:

(i) Christabel Corporate Services Limited, 118 Agias Fylaxeos, Christabel House, 3087 Limassol, Cyprus

(ii) Christabel Support Services Limited, 118 Agias Fylaxeos, Christabel House, 3087 Limassol, Cyprus

For privacy matters and GDPR related issues the contact email of CHRISTABEL is privacy@christabelonline.com.

CHRISTABEL DATA PROTECTION POLICY

The present Privacy Policy is comprised of two main parts:

(i) **PART I:** Our Privacy Commitments; and

(ii) **PART II:** CHRISTABEL's System of Management of Personal Data.

To comply with the above legal requirements and the laws relating to the collection, processing, storing, transferring and generally handling of personal data CHRISTABEL has implemented, internally and uniformly, the present DATA PROTECTION POLICY (hereby referred to as '**the Privacy Policy**'), to ensure that CHRISTABEL is compliant with all relevant laws and regulations.

In addition to this Privacy Policy, we took the following several other steps to ensure compliance with the GDPR:

(i) performed a data flow audit;

(ii) amended agreements or drafted new agreements where it was necessary;

(iii) drafted consent forms attached to agreements, even if the processing and collection was lawful, and in particular, where 'sensitive data' had to be collected for our employee recruitment process or for the performance of a contract, such as the provision of corporate services;

(iv) demonstrated compliance through our website where there is a website Privacy Policy;

(v) provided awareness seminars/trainings for our employees;

(vi) set up data breach safeguards, procedures and implemented data protection governance;

(vii) Appointed an accountable executive as our Data Protection Officer.

Our Privacy Policy is comprehensive, clear and transparent.

The principle of accountability is a cornerstone of the GDPR and CHRISTABEL's Privacy Policy demonstrates commitment to accountability. All CHRISTABEL employees and entities have a responsibility to follow and abide by this Privacy Policy, irrespective of geographic location, and have been professionally trained for this purpose.

However, should you have any questions or queries regarding our Data Protection Policy, please send an email to privacy@christabelonline.com

PART I: OUR PRIVACY COMMITMENTS

PRIVACY COMMITMENT 1: COMPLIANCE WITH PRIVACY LAWS

At CHRISTABEL, we respect the privacy of our employees, clients, vendors and business partners. We are committed to managing personal data in a professional, lawful and ethical manner. We comply with applicable data protection laws and regulations including the EU GDPR.

(a) Data protection laws safeguard the 'personal data' of 'data subjects'.

In this privacy policy, your data is sometimes referred to as "personal data" or "personal information". We may also sometimes collectively refer to handling, collecting, protecting and storing your personal data or any such action as "processing" such personal data.

Consent shall mean any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Data Controller – the entity that determines the purposes, conditions and means of the processing of personal data

Data Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subjects are identifiable living persons who provide their personal data to a business, company or organization. They include employees, partners and clients.

Personal data is any information that relates to an identified or identifiable living individual**.** Different pieces of information, which collected together and lead to the identification of a particular person, also constitute personal data.

EXAMPLES based on the case and purpose of the processing including but not limited to:

- Name, Gender, Date of Birth, Age, Nationality, Citizenship;
- Home/Work Postal Address, Home/Work landline phone number, Home/Work mobile phone number, Personal/Work email address;
- Source of Funds and Source of Wealth, information on financial transactions (where applicable), Tax Residency information;
- Information on education and employment of the individual and information on any potential political involvement of the individual;

  Records of any Correspondence with the individual;
- Information and/or documentation that we are required to request and obtain for the purposes of our Know Your Client procedures and Anti – Money Laundering law and regulations;

- Information you provide to us for the purposes to attending meetings and/or events, including dietary requirements which may reveal information about your health or religious beliefs.
- Social Insurance No.
- Passport and/or Identity Card
- Bank account details

The processing of **'sensitive' personal data** requires the explicit consent of the individual or processing is allowed under a demonstrated **lawful basis.**

CHILDREN'S DATA

The processing of the personal data of a child shall be lawful where the child is at least 14 years old. Where the child is below the age of 14 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.
Parental consent form is hereby attached as **Appendix A** to this policy.

Process, Processed, Processing shall mean in accordance with the GDPR any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include the following:

- collection;
- recording;
- organization;
- structuring;
- storage;
- adaptation or alteration;
- retrieval;
- consultation;
- use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination;
- restriction;
- erasure or destruction.

In fulfilling our contractual and legal/regulatory obligations, your personal data may be given to various departments of the Company. Various service providers and suppliers as seen below may also receive your personal data in order to fulfil our obligations and provide our services. These service providers and suppliers enter into contracts with the Company in which they are contractually bound by confidentiality as well as data protection as per the local data protection legislation and the GDPR:

- applicants for employment (including speculative applicants);

- employees;
- clients;
- banks, financial institutions and any other similar organizations that are nominated by the Client;
- auditors;
- accountants;
- agents;
- lawyers/advisors;
- Companies providing services such as packaging, mailing and delivery purchases, postal mail etc;
- any organization at the Client's request or any person acting on behalf of the client;
- any third parties where this is necessary to process a transaction or provide services which the client has requested.
- other companies;
- institutions in other countries.
- Various government platforms such as "Ariadni" or other companies for the purposes of performing Know Your Customer (KYC) verification, provided your prior consent has been obtained;

(b) Complying with the CHRISTABEL Privacy Policy

We require that all CHRISTABEL employees who collect, use and store personal data understand privacy rules and their responsibilities when processing personal data. We also require that all CHRISTABEL employees understand how to respect and manage individuals' rights in relation to their data.

The CHRISTABEL Privacy Policy applies to all:

(i) personal data processed by us, regardless if we process the data ourselves or if we have outsourced the data to a third-party controller or stakeholder;

(ii) personal data, regardless if they relate to our employees, customers, vendors, business partners, or any other stakeholder we communicate or deal with; and

(iii) electronic processing of personal data and processing in systematically accessible paper-based filing systems (e.g. in an organized cabinet).

(iv) Personal data of natural persons who currently have or who previously had a business relationship with the Company,

PRIVACY COMMITMENT 2: PROCESSING PERSONAL DATA FOR LEGITIMATE PURPOSES

LAWFUL PROCESSING (Articles 6 to 10 of the GDPR)

CHRISTABEL only processes personal data for specified and lawful purposes which are clearly explained to individuals when we process their data. Below we represent the legal grounds and the legitimate purposes for which we process personal information of employees and other individuals. These overviews are intended to be a generic summary. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if the purpose can reasonably be achieved by some other less intrusive means, or by processing less data.

Lawful Processing means that CHRISTABEL will not process personal data, unless one of the following conditions applies:

(i) perform, or take steps with a view to enter into, a contract with the relevant individual, partner or client;

(ii) comply with a legal obligation to which CHRISTABEL is subject; This includes amongst others: Anti money – laundering law, ASP Law. Tax legislation, Companies' law.

(iii) Protect the vital interests of the individual, partner or client concerned; we process personal data in order to ensure the legitimate interests pursued by us or by third parties. A legitimate interest exists when we have a business or commercial reason for using your information. But, even then, you should not unreasonably oppose what is right and best for you. Examples of such processing activities include the following:

- Establishing legal claims and preparing our defence in litigation;

- Means and procedures we undertake to ensure the security of the IT Department and the Company's systems, to prevent data leakage, prevent potential criminal acts and fraud, secure assets, access control and anti-breach measures .

- Installation of surveillance systems (closed-circuit cameras – CCTV)

- Measures to manage tasks such as centralizing the management of customer correspondence, and to further develop services;

- Use of external investigative consultants and/or other intelligence services for the purpose of conducting further investigations of customers who pose an increased risk in relation to money laundering/terrorist financing and where it is deemed necessary to take enhanced due diligence measures;

- Processing of personal data of third parties in the context of issuing letters of guarantee concerning these third parties,

- The delegation of communication between the Company and its customers e.g. calls and/or correspondence by post and/or electronic correspondence to third party service providers;

- Provision of your personal data to the responsible government authorities in relation to various government schemes.

- Carrying out enhanced due diligence measures in relation to existing customers where it is suspected that the customer's country of origin or residence is a sanctioned country;

- Processing your personal data for marketing purposes using specialized tools, which includes profiling;

(iv) The individual, partner or client concerned has consented to the processing (especially regarding the processing of 'sensitive' personal data); where you have given us your express consent to processing (other than for the reasons set out above), the lawfulness of such processing is based on that consent. You have the right to withdraw your consent at any time. However, any processing of personal data carried out prior to receipt of your revocation is not affected.

(v) in circumstances permitted by applicable data protection laws.

CHRISTABEL will not use data for new purposes without following our internal procedures to verify that such processing can take place lawfully.

CONSENT (Article 7 of the GDPR – on conditions for consent)

If applicable law requires this, CHRISTABEL shall obtain consent from the individual.
Where the individuals ask for the processing of personal data, they will be deemed to have given consent. For the avoidance of any doubt, Christabel shall receive explicit consent for the processing of data of individuals.

When asking consent, CHRISTABEL shall inform the individual:

(a) of the purposes of the processing for which consent is required; and

(b) other relevant information as set out under Privacy Commitment 8 (e.g. the categories of personal data, the categories of third-parties receiving personal data and how individuals can exercise their rights).

CHRISTABEL shall inform individuals that they may both refuse consent and withdraw a given consent at any time. Withdrawal of a given consent will not affect the lawfulness of the processing based on such consent before its withdrawal.

EMPLOYEE CONSENT

If applicable law requires it, CHRISTABEL shall also ask employee consent for the processing of their personal data, especially where such data include special categories of data, or if the processing and monitoring occurs in a regular and systematic manner (for example, the use of CCTV at our premises).
When asking for their consent, CHRISTABEL shall additionally inform employees:

a) of the possible consequences of the processing; and

b) that they are free to refuse to withdraw consent at any time without consequence to their employment relationship.

Employees consent form is hereby attached as **Appendix B.**

CCTV (closed circuit television system) surveillance

Installation of a CCTV system is installed at our premises. All for reasons relating to the subject's personal safety and integrity and as precautionary/preventive measures against theft, to protect our Company's assets and resources; and, mostly, to ensure the life, safety and integrity of our people. Surveillance equipment shall not be used for the purpose of regular monitoring of employees in the workplace. In Christabel's premises surveillance equipment is NOT installed in offices, conference rooms, corridors, kitchen, or restrooms. The only person who has access to the footage of the premises is the Managing Director of CHRISTABEL, Mr. Christos Ioakim. Employees that are monitored and under the surveillance have given their explicit consent and have been told about the recording and their rights under the GDPR. Signs of the cameras within the premises are dully displayed at all times. Data must only be kept for a reasonable amount of time.

LAWFUL PROCESSING OF SENSITIVE DATA (Article 9 – on the processing of special categories)

CHRISTABEL sometimes processes sensitive data.

Sensitive data are personal data that reveal an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural personal, data concerning health or data concerning a natural person's sex life or sexual orientation (*Article 9 of the GDPR 'Processing of special categories of personal data'*).

CHRISTABEL will not use or process sensitive personal data for any purposes without following our internal procedures to verify that such processing can take place lawfully.

Sensitive data enjoy more protection than regular personal data. CHRISTABEL will treat any collection, use or storage of sensitive data with more scrutiny as such data requires additional privacy, legal and security safeguards. Where the processing of genetic and biometric data is based on a data subject's consent, the further processing of such data requires the separate consent of the data subject.
When the controller or the processor intends to transfer special categories of personal data to a recipient in a third country or to an international organisation and the intended transfer is based on appropriate safeguards provided for in Article 46 of the GDPR or on binding corporate rules ('BCRs') provided for in Article 47 of the GDPR, the controller or processor must inform the Commissioner of the intended transfer before the data is transferred

CHRISTABEL may process categories of sensitive data if necessary and subject to the regulation:

(i) where the individual concerned has given their explicit consent that we may do so, based on a full understanding of why data is being collected;

(ii) for the performance of a task carried out to comply with or allowed by law;

(iii) to comply with any law and/or court order and/or orders of a regulatory authority;

(iv) for the establishment, exercise or defence of a legal claim;

(v) to protect a vital interest of an individual, but only where it is impossible to obtain the individual's consent first;

(vi) to the extent necessary for reasons substantial of public interest;

(vii) for recruintment purposes.

If none of the above legitimate purposes apply, please see below the more specific legitimate purposes to process sensitive data of employees and other individuals.

USE OF PERSONAL DATA FOR OTHER PURPOSES THAN THE ORIGINAL

It is only allowed to process personal data for a purpose other than the original legitimate purpose for which the personal data were collected if the original purpose and the secondary purpose are closely related. In this case you should contact the relevant data protection officer at privacy@christabelonline.com. Depending on the sensitivity of the relevant personal data whether the secondary purpose has potential negative consequences for the individual, the secondary use may require additional measures such as:

(a) limiting access to the data;
(b) imposing additional confidentiality requirements;
(c) taking additional security measures;

(d) informing the individual about the secondary purpose;
(e) providing an opt-out opportunity; or
(f) obtaining an individual's consent.

PRIVACY COMMITMENT 3: ACCOUNTABILITY AND RISK ASSESMENT

ACCOUNTABILITY, POLICIES AND PROCEDURES

Everyone who works for or on behalf of CHRISTABEL is responsible for processing personal data ethically, lawfully and in accordance with the present Policy. Everyone is expected to:

(i) comply with the CHRISTABEL policies and data protection guidance when processing personal data,

(ii) understand the data protection requirements which have relevance to the personal data they process on behalf of CHRISTABEL using our policies, guidance and training material, and

(iii) follow our processes and comply with our procedures and measures.

CHRISTABEL has processes and procedures in place to manage its compliance and monitoring in accordance with data protection requirements. We have appropriate technical and organizational measures to meet these requirements and have amended and updated our contractual agreements to meet the requirements of data protection accordingly.

RECORD KEEPING

CHRISTABEL maintains electronic records and evidence of its data processing activities and compliance, in the event that we need to show individuals, auditors, supervisory authorities, other public authorities and clients how we meet our obligations. These records are held and maintained by different functions with regular reporting channels to the members of the team responsible for checking compliance with the CHRISTABEL Privacy Policy and our data protection procedures. Our employees understand that they are accountable for maintaining evidence and records where these responsibilities are applicable to their roles.

DATA PROTECTION IMPACT ASSESMENT

CHRISTABEL shall conduct a Data Protection Impact Assessment (hereby referred to as '**DPIA**') prior to the processing if it is likely to result in a high risk to the rights and freedoms of individuals. Everyone at CHRISTABEL is obliged to contribute to a DPIA if they are asked to.

A DPIA is a review procedure to carry out and document an assessment of the impact of any new system or management of processing on the protection of personal data and privacy rights. The DPIA will be performed prior to the implementation of a new system or management of processing and will regard the entire lifecycle management of personal data, from collection to processing to deletion. A DPIA contains a description of:

(a) the relevant CHRISTABEL entities and third parties responsible for the processing;

(b) the envisaged processing;

(c) the purpose for which personal data are processed;

(d) security measures;

(e) data retention periods;

(f) categories of recipients;

(g) any transfers of personal data out of the EEA, including suitable transfer mechanisms;

(h) and an assessment of the necessity and proportionality of the envisaged processing, the risks to the privacy rights of individuals including a description of mitigating (privacy by-design and privacy by- default) measures to minimize these risks and the context of processing.

The outcome of a DPIA is to identify the necessary measures to minimize risk and comply with applicable data protection law and the GDPR. CHRISTABEL will consult with the competent data protection authority prior to processing taking place when required to do so. Not all processing requires a DPIA. In these instances, CHRISTABEL has a process to initiate privacy reviews to assess our own practices, service offerings, technology to mitigate risks and allow for privacy integration through measures such as privacy by design or adopting privacy as the default setting. The outcome of a privacy review may also be the need for a DPIA.

CHRISTABEL has internal processes in place to manage DPIAs and privacy reviews. All entities are required to act on the outcome of a DPIA or review to help mitigate any privacy risks, including implementing additional measures to mitigate those risks.

For the ease of reference a guideline chart for the approach to be taken when making a data protection impact assessment has been created and is attached hereto as **Appendix C**.

PRIVACY COMMITMENT 4: CONFIDENTIALITY, SECURITY AND MEASURES FOR BREACH INCIDENTS

DATA SECURITY

CHRISTABEL shall take appropriate commercially reasonable technical and organizational measures to protect personal data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access or other processing.

IT MAINTENANCE AND SECURITY

CHRISTABEL is party to a contract agreement with the IT provider, A.X.C. PROFESERV LTD, who is responsible under the agreement to follow the GDPR and ensure that no breach occurs, and data is safely stored, transferred and processed.

For our database and crewing management, we use the safe and secure Meraki Security Device, as the firewall. Additionally to the firewall, all computers are protected with the ESET Endpoint Antivirus which ensures a secure database, including but not limited to password scrambling, anonymization procedures for sensitive data (Security Attribute functionality), database parameters and other customizations. Our IT providers ensure offsite and onside back-ups on a regular basis and guarantee the offsite disaster recovery of the data.

In addition to the above, all our computers used by our employees at our premises have individual and complex passwords and each computer is accessible only by one employee at a time.

STAFF ACCESS

Staff members will be allowed to access personal data only to the extent necessary to serve the applicable legitimate purpose and to perform their job. There are protocols in place to prevent unauthorized access and where appropriate, we have access control procedures to limit access to personal data to authorized individuals. Where relevant, we observe restrictions on disclosures applicable under relevant laws, contractual arrangements or relevant to CHRISTABEL's processing including when we share data with vendors and partners.

Staff members who access personal data will meet their confidentiality obligations as per the employee handbook initially provided to the employee upon his/her employment.

DATA SECURITY BREACH NOTIFICATION REQUIREMENT

CHRISTABEL has policies, procedures and protocols in place for managing and responding to data security breaches. All instances of suspected or known breaches where there may have been inappropriate access to or an unauthorized disclosure of personal data must be reported immediately to the GDPR officer of CHRISTABEL and by email to privacy@christabelonline.com. All employees are required to follow our security instructions. There are notification procedures for reporting the breaches internally and externally to supervisory authorities and individuals. *Article 33 of the GDPR provides that within 72 hours of the event of breach of personal data the controller of personal data should notify the relevant supervisory authority.* This should be without undue delay where the breach is likely to cause significant risks to the individual.

CHRISTABEL maintains a record of data security breaches which includes details about the breach incident, the effects (if any) on individuals, CHRISTABEL or any other party, and remedial action necessary to resolve the breach. CHRISTABEL will make these records available to the relevant supervisory authority if requested to do so.

CHRISTABEL shall notify individuals of a data security breach if the breach is likely to result in a high risk to an individual's rights and freedoms. A data security breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data security breach notification form is hereby attached as **Appendix D**.

PRIVACY COMMITMENT 5: GENERAL TREATMENT OF PERSONAL DATA

NO EXCESSIVE PROCESSING OF PERSONAL DATA

CHRISTABEL has procedures in place to only collect and process personal data that is relevant and reasonably required to achieve a specific purpose. Where feasible and appropriate, we consider using anonymous, pseudonymized or aggregated data instead of personal data. We also take reasonable steps to delete personal data that are not required for the applicable purpose.

LIMITED STORAGE PERIOD

CHRISTABEL does not retain personal data for longer than necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the purposes they were obtained or in accordance with legal/regulatory specified retention requirements.

With no prejudice on the above, our retention period is currently at five (5) years after the completion of any formal relations with the Company. Should data subjects request the deletion of such data and provided that there is no legal requirement to which the Company must comply to the relevant data will be safely deleted or destroyed. This also applies to those cases in which your relationship for any reason with Christabel is interrupted.

Promptly after the applicable storage period has ended, the relevant HR manager shall direct that the personal data be:

(a) securely deleted or destroyed,

(b) anonymized, or

(c) transferred to an archive (unless this is prohibited by law or an applicable records retention schedule).

CHRISTABEL proceeds to always shredding any printed documents containing personal data and irreversibly destroy any personal data both hard copy and digital form we have in our possession whereas such information is no longer needed.

CHRISTABEL has controls, procedures and systems to verify that personal data is accurate, up to date and relevant to achieve a specific purpose. Electronic documents are kept in a passcode encrypted software again with limited access to responsible employees.

ACCURATE, COMPLETE AND UP-TO-DATE PERSONAL DATA (DATA QUALITY)

CHRISTABEL has controls, procedures and systems to verify that personal data is accurate, up to date and relevant to achieve a specific purpose.

PRIVACY BY DESIGN – BUILDING PRIVACY INTO OUR CONTRACTS, PROCEDURES AND PROJECTS

CHRISTABEL considers data protection as an integral component of the design, development, operation and management of new projects, tools, applications, internal services and offerings, which process personal data. To this end, there is internal guidance and processes on how to incorporate privacy as an essential part at the beginning of the design and development stages. When CHRISTABEL engages employees, vendors, partners and agencies as part of any design, development and implementation work, we have procedures in place to ensure privacy by design is an integral component.

PRIVACY BY DEFAULT – CHOOSING THE PRIVACY FRIENDLY OPTION

CHRISTABEL will use or adopt privacy as the default setting when designing or implementing new projects, procedures and business activities.

PRIVACY COMMITMENT 6: TRANSPARENCY OF PRIVACY PRACTICES

CHRISTABEL provides individuals with information. Notices and statements are written in accordance with CHRISTABEL guidance and include all relevant information necessary to meet our regulatory obligations and ensure fair and lawful processing. The information is made easily accessible to individuals and is provided in a clear, transparent manner using plain and intelligible language.

An individual has the right to know about CHRISTABEL's processing of their personal data and to verify whether the processing is lawful. CHRISTABEL informs individuals through the privacy notice attached hereto as **Appendix E** about:

(a) the purposes for which we intend to use such data including the legal basis for processing the data;

(b) whether we are required or obliged to process such data with reference to a legal obligation where applicable;

(c) the recipients or categories of recipients of the data;

(d) whether there is a necessity to transfer such data within or outside the EEA;

(e) their rights under the GDPR and how these rights may be exercised.

USING PERSONAL DATA FOR NEW PURPOSES

CHRISTABEL will make sure that information to individuals is also provided in all instances where existing personal data is going to be used in a new way, or for different purposes prior to the commencement of such processing always subject to Recital 50 of the GDPR

PRIVACY COMMITMENT 7: DISCLOSURE SAFEGUARDS TO THIRD PARTIES AND TRANSFERRING ABROAD

TRANSFER TO THIRD PARTIES

CHRISTABEL recognizes that adequate protection is important where it provides personal data to third parties outside of its group. A transfer of personal data will include situations in which CHRISTABEL discloses personal data to any third party or where CHRISTABEL provides remote access (e.g. in the context of corporate due diligence).

There are two categories of third parties:

(1) third party controllers: these are third parties that determine the how and for what reason personal data are processed (purposes and means of the processing).

(2) third party processors: these are third parties that process personal data only on behalf of CHRISTABEL and only under its instruction.

THIRD PARTY DATA CONTROLLER SAFEGUARDS

Third party controllers may process personal data only if they have a written contract with CHRISTABEL. In this contract, CHRISTABEL safeguards the data protection interests of individuals. All contracts with third party controllers should be concluded in consultation with our legal consultants.

In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
The controller may be exempted, in whole or in part, of the obligation to communicate a personal data breach to the data subject, for one or more purposes referred to in Article 23(1) of the GDPR. The exemption from the obligation for data breach notification requires a DPIA and prior consultation with the Commissioner. The DPIA shall include the information set out in Articles 23(2) and 35(7) of the GDPR. The Commissioner may impose terms and conditions on the controller for the exemption (Article 12 of the Law).
Data controllers in certain sectors may be required to inform sectoral regulators of any breach.

THIRD PARTY PROCESSOR CONTRACTS

Third party processors may process personal data only if they have a written contract with CHRISTABEL. The contract with a third-party processor will include the following provisions:

(a) the processor shall process personal data only in accordance with CHRISTABEL's documented instructions and for the purposes allowed by CHRISTABEL;

(b) the processor shall ensure that its personnel which processes personal data keeps the personal data confidential;

(c) the processor shall take appropriate technical, physical and organizational security measures to protect personal data;

(d) the processor shall not permit subcontractors and affiliates to process personal data without the prior written consent of CHRISTABEL;

(e) the processor shall ensure that its subcontractors and affiliates abide by a level of data protection no less protective than the obligations as set out in the contract between processor and CHRISTABEL;

(f) CHRISTABEL may review the security measures taken by the processor and the processor shall submit its relevant data processing facilities to audits and inspections by CHRISTABEL, to a third party on behalf of CHRISTABEL or any relevant governmental authority;

(g) the processor shall promptly inform CHRISTABEL of any actual or suspected security breach involving personal data;

(h) the processor shall take adequate remedial measures following a data security breach and shall promptly provide CHRISTABEL with all relevant information and assistance as requested by CHRISTABEL regarding the security breach; and

(i) at the choice of CHRISTABEL, the processor shall delete or return all personal data to CHRISTABEL at the end of the provision of services relating to the processing of personal data and shall delete all copies of the personal data, unless storage of the personal data is required by applicable law.

TRANSFER OF PERSONAL DATA OUTSIDE OF THE EEA

Privacy laws place restrictions on transfers of personal data across borders for any type of processing (collection, use, storage etc.). These restrictions also apply to internal transfers of personal data within CHRISTABEL across the countries where we operate, and to transfers of personal data to vendors, agencies, partners or other third parties located in different countries.

CHRISTABEL will only transfer personal data outside the EEA if:

(a) the transfer is necessary for the performance of a contract, for managing a contract or to take necessary steps prior to entering into contract;

(b) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between CHRISTABEL and the individual or between CHRISTABEL and a third party in the interest of all parties concerned;

(c) the third party has implemented transfer control mechanisms and other security and organizational measures which provides adequate safeguards under applicable law;

(d) the transfer is necessary for the establishment, exercise or defense of a legal claim;

(e) the transfer is necessary to satisfy an important reason of public interest;

(f) the transfer is necessary for the performance of a task carried out to comply with or allowed by law to which CHRISTABEL is subject;

(g) the transfer is necessary for the health and safety of CHRISTABEL employees.

CONSENT FOR TRANSFER

If none of the grounds exist or if applicable law so requires CHRISTABEL may (also) request consent from the individual for the transfer to a third party located outside the EEA. Prior to requesting consent, the individual will be provided with the following information:

a) the purpose of the transfer;

b) the identity or categories of third parties to which the personal data will be transferred;

c) the categories of personal data that will be transferred; and

d) the fact that the personal data will be transferred to a country that does not have an adequate level of data protection.

NON-REPETITIVE TRANSFERS

Where none of the above-mentioned grounds to transfer apply, the transfer may take place when:

(a) that transfer is not repetitive;

(b) the transfer concerns a limited number of individuals;

(c) the transfer is necessary for a compelling legitimate interest of CHRISTABEL which does not override the rights and freedoms of the individual; and

(d) CHRISTABEL has implemented suitable safeguards to protect the personal data.

A transfer for a non-repetitive transfer needs to be approved by CHRISTABEL's GDPR officer. CHRISTABEL shall inform the individual of the relevant data protection authority of the transfer and, to the extent necessary under applicable law, obtain the consent of the individual.

PRIVACY COMMITMENT 8: THE PRIVACY RIGHTS OF INDIVIDUALS

Individuals have rights in relation to their personal data processed by CHRISTABEL. We respect the privacy of our clients and have ensured to implement procedures and practises to recognize and respond to individuals wishing to exercise these rights. Our employees, or anyone acting on behalf of CHRISTABEL, have guidance in relation to individuals' rights. These rights are:

THE RIGHT TO BE INFORMED (Article 13 and 14 of the GDPR)

This right has been covered in detail in "Privacy Commitment 6".

The provisions of Article 14 of the GDPR shall apply to the extent that they do not affect the right to freedom of expression and information and the press confidentiality (Article 29(2) of the Law).

ACCESS TO THEIR PERSONAL DATA PROCESSED BY CHRISTABEL (Article 15 of the GDPR)

The provisions of Article 15 of the GDPR shall apply to the extent that they do not affect the right to freedom of expression and information and the press confidentiality (Article 29(2) of the Law).

An individual has the right to request access to the personal data we process about them. When CHRISTABEL receives such request, will take reasonable steps to:

(a) identify the individual making the request;

(b) decide whether CHRISTABEL is processing their personal data; and

(c) where we process large amounts of personal data, ask for specific information to help locate that personal data.

As requested, CHRISTABEL will provide the individual with the following information:

(a) purposes of the processing

(b) if data is held, together with an indication of the source(s) of the data if known;

(c) the categories of personal data;

(d) the recipients of the data, including recipients in other countries and details of the appropriate safeguards in place for the transfer of their data to other countries;

(e) if applicable, any automated decision-making or profiling applied to the personal data and the significance of such processing; and

(f) how long the data will be retained or the retention criteria.

CHRISTABEL will inform the individual regarding their rights in case there is a request of rectification, erasure, restriction on use of the data by CHRISTABEL, or their right to lodge a complaint with a supervisory authority.

CHRISTABEL will provide this information and these copies within one month of receiving an individual's request, or within any specific period that may be required by local law in any country. Where the request has been made electronically, CHRISTABEL will provide the information in a commonly used electronic format.

CHRISTABEL may, however, refuse to provide an individual with information where disclosure of that information would reveal information about another individual (in which case CHRISTABEL will provide as much as possible without revealing information about the other individual), unless the other individual agrees that CHRISTABEL may release the information or CHRISTABEL decides that it is reasonable to provide the information without the other individual's consent.

CHRISTABEL may refuse to comply with a request but will explain our reasons for doing so to the individual and inform them of their right to complain to a supervisory authority and/or seek judicial remedy within one month (with the potential of extension if the request is complex or we have received a number of requests from the specific individual by providing prior notice and explaining why the extension is necessary.) of receiving our refusal to comply with the request. In addition, in some countries localized guidance may provide other legitimate reasons for refusing an individual's request for access, in accordance with local data protection law.

THE RIGHT TO RECTIFICATION (Article 16 of the GDPR)

An individual may request that CHRISTABEL rectify their personal data if the data is inaccurate or incomplete:

(a) if CHRISTABEL has disclosed the data to a recipient, we will inform the recipient of the request where feasible to do so. An individual may request information about the recipients from CHRISTABEL;

(b) if CHRISTABEL agrees that the data is incorrect, we will delete or correct the data;

(c) if we do not agree that the data is incorrect, CHRISTABEL will inform the individual and explain their right to complain to a supervisory authority and to seek judicial remedy.

CHRISTABEL will keep a record that the individual considers the data to be inaccurate or incomplete.

THE RIGHT TO ERASURE (THE RIGHT TO BE FORGOTTEN) Art. 17 GDPR

CHRISTABEL will abide by a request from an individual to erase their personal data under the following conditions as specified within privacy laws:

(a) the personal data is no longer necessary for the purpose for which they are collected or otherwise processed;

(b) the individual withdraws consent and there are no other legal grounds for processing;

(c) the individual objects to the processing and we have no overriding legitimate interests for continuing to process their data;

(d) the personal data is being unlawfully processed;

(e) the data must be erased to comply with a legal obligation applicable to CHRISTABEL as a data controller.

There are circumstances when CHRISTABEL can refuse an erasure request. These reasons include:

(a) exercising the right of freedom of expression and information;

(b) complying with a legal obligation applicable to CHRISTABEL as a data controller or the performance of a public interest task or exercise official authority;

(c) for public health reasons or for purposes in the public interest;

(d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes, or for the establishment, exercise or defence of legal claims.

CHRISTABEL will inform any recipients about the erasure request unless this would require a disproportionate effort. Where CHRISTABEL has made the data public, it will take reasonable steps (taking into account cost and technology) to inform other recipients of the data to erase links to, copies or replication of, those personal data. CHRISTABEL will comply with any specified timeframes for complying with such requests.

THE RIGHT TO RESTRICT PROCESSING (Article 18 of the GDPR)

CHRISTABEL will agree to restrict the processing of an individual's data when one of the following conditions applies:

(a) if the individual contests, the accuracy of the data, CHRISTABEL will restrict using the data until the accuracy can be verified;

(b) the processing is unlawful and the individual requests a restriction of use rather than erasure of their data;

(c) CHRISTABEL no longer needs to process the personal data but the individual requires the data to establish, exercise or defend a legal claim;

(d) in circumstances where an individual has objected to the processing (which was necessary for purposes in the public interest or CHRISTABEL's legitimate interests) and CHRISTABEL is considering whether CHRISTABEL's interests override the rights of the individual.

If there is a restriction on processing, CHRISTABEL has the right to retain the data but will not process it any further.

CHRISTABEL will inform any recipients of the personal data about the restriction unless it is disproportionate to do so. An individual can request information about the identity of the recipients from CHRISTABEL. If CHRISTABEL lifts the restriction on processing it will inform the individual.

THE RIGHT TO PORTABILITY (Article 20 of the GDPR)

An individual has the right to request portability of personal data which they provide to CHRISTABEL if:

(a) the processing is based on the individual's consent or for the performance of a contract; and

(b) the processing is automated.

The right applies to data that an individual has provided to CHRISTABEL. If the personal data includes data about other individuals, CHRISTABEL will take steps to erasure providing the information would not affect the rights and freedoms of other individuals.

CHRISTABEL will:

(a) provide the information free of charge and in a structured, commonly used and machine-readable format;

(b) transfer the information directly to another data controller at the request of the individual, where technically feasible;

(c) respond to the request within one month;

(d) notify the individual if we cannot respond within one month, explaining the reasons for the delay and notify them of this within one month of receiving the request;

(e) respond within two months where a request has been delayed;

(f) inform an individual within one month of receiving their request if it cannot respond to such a request and inform them of their right to make a complaint to the supervisory authority and/or seek judicial review.

THE RIGHT TO OBJECT (Article 21 of the GDPR)

An individual has the right to lodge an objection (under certain circumstances) to processing of their data by CHRISTABEL. CHRISTABEL will abide by any valid request from an individual who objects to the processing of their data by CHRISTABEL.

Under certain circumstances, there may be grounds for CHRISTABEL to continue certain types of processing where we can demonstrate that our legitimate interests override the rights of an individual or in instances where the processing is necessary for the establishment, exercise or defence of legal claims.

CHRISTABEL will respond to a request within the specified timeframe. Where we cannot process the objection, we will notify the individual and explain the reasons why.

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING (Article 22 of the GDPR)

An automated decision is when a decision is made about an individual using technology specifically designed for decision-making purposes. This includes profiling individuals. Under the GDPR, an individual has the right NOT to subject to solely automated decisions which produce legal effects or significantly affect them, which may result in adverse consequences for an individual. An individual has the right to ask for an explanation of the decision, offer their opinion and challenge the decision.

The right does not apply, where the decision is:

(a) made with the explicit consent of an individual;

(b) for the purposes of a contract; or

(c) Permitted by law.

Where consent or contracts are relied upon, there must be suitable safeguards such as human intervention to review the decision in order to protect the individual. There are restrictions on making automated decisions using personal data. CHRISTABEL will comply with the relevant requirements when making automated decisions and will institute any additional safeguards to protect individual's rights where required to do so. Christabel must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

THE RIGHT TO COMPLAIN TO A SUPERVISORY AUTHORITY (Article 77 of the GDPR)

An individual shall have the right to lodge a complaint with CHRISTABEL under the following circumstances:

(a) the response to the request is unsatisfactory to the individual (e.g. the request is denied); or

(b) The individual has not received a timely response.

DENIAL OF REQUESTS

CHRISTABEL may deny an individual request under the following circumstances:

(a) the request does not meet the requirements set to it;

(b) the request is not sufficiently specific or manifestly unfounded;

(c) the identity of the relevant individual cannot be established by reasonable means; or

(d) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights. A time interval between requests of six months or less will generally be deemed to be an unreasonable time interval.

THE RIGHT TO WITHDRAW CONSENT (Article (3) of the GDPR)

You have right to withdraw the consent that you have given to the Company with regard to the processing of your personal data at any time. Note that any withdrawal of consent shall not affect the lawfulness of processing based on consent before it was withdrawn or revoked by you.

You can also contact our Data Protection Officer at privacy@christabelonline.com

We endeavour to address all of your requests promptly

Cyprus Law exceptions to data subject rights

In cases where it is necessary to safeguard GDPR Article 23 objectives, the Personal Data Law permits controllers to vary or restrict the below mentioned data subject rights:

Data Breach notification obligations (Article 34 GDPR)
Data portability right (Article 20, GDPR)
Notification obligation relating to rectification and erasure requests (Article 19, GDPR)
Processing restriction right (Article 18, GDPR)
Transparency obligations (Article 12, GDPR)

Pursuant to GDPR Article 14(5), the controller shall inform data subjects regarding any restrictions to their rights

Commissioner may impose certain terms on the Controller in regards to any restrictions imposed by the controller and/or the information provided to the data subject pursuant to the Personal Data Law.

PRIVACY COMMITMENT 9: STAFF TRAINING

STAFF TRAINING

All CHRISTABEL employees who regularly process personal data will be given appropriate and timely data protection training. If required to do so, CHRISTABEL will provide the supervisory authorities with examples of our training program. Relevant information regarding privacy rules will be communicated in a clear and accessible manner to all our employees.

PART II: CHRISTABEL'S SYSTEM OF MANAGEMENT OF PERSONAL DATA

CHRISTABEL's Privacy Policy addresses the processing of personal data of executives, employees, suppliers, business partners and other individuals and third parties by CHRISTABEL or a third party on behalf of CHRISTABEL.

This code applies to the processing of personal data by electronic means and in systematically accessible paper-based filing systems.

This code will not apply to the processing of personal data collected in connection with activities of a CHRISTABEL entity located in a non-adequate country, with the exception of the security and governance requirements of this code which will remain applicable. In respect of such processing of personal data, the relevant CHRISTABEL entity may decide whether to apply this code. Such processing of personal data will at least be compliant with applicable local data protection laws.

CHRISTABEL's Privacy Policy has been adopted by the directors of CHRISTABEL. It has entered into force as of the following effective date: **25 May 2018** and has been reviewed and updated as of **1st of July 2022** It will be shared within the CHRISTABEL companies; all employees will have access to it and will be made available to supervisory authorities and to individuals upon request.

CHRISTABEL's Privacy Policy will supersede all CHRISTABEL's privacy policies and notices that exist as of the effective date to the extent they are in contradiction with the CHRISTABEL Privacy Policy. All relevant contract agreements will be amended in order to be in accordance with the CHRISTABEL Privacy Policy.

GOVERNANCE

The governance of this code is carried out by the following roles:

(a) the accountable executive who will be responsible for compliance with this code within the relevant CHRISTABEL operating company;

The specific responsibilities of each role are further set our below.

THE ACCOUNTABLE EXECUTIVE (DATA PROTECTION OFFICER)

The accountable executive will be accountable for the implementation of effective data protection management, the integration of effective data protection into business practices, and that adequate resources and budget are available. Accountable executives will be accountable for:

(a) ensuring overall data protection management compliance within CHRISTABEL, also during and following organizational restructuring, outsourcing, mergers and acquisitions and divestitures;

(b) implementing the data management processes, systems and tools devised to implement the framework of data protection management across CHRISTABEL companies.

(c) ensuring that the data protection management processes and systems are maintained up to date against changing circumstances and legal and regulatory requirements in cooperation with our legal consultants;

(d) ensuring and monitoring on-going compliance of third parties with the requirements of the CHRISTABEL Privacy Policy in case personal data are transferred by CHRISTABEL to a third party (including entering into a written contract with such third party and obtaining a sign off of such contract);

(e) ensuring the awareness-raising and training regarding the data protection regulations of the relevant individuals in their organizational unit
(f) directing stored data to be deleted or destroyed, anonymized or transferred as required by our value treating data with care; andPursuant to the Personal Data Law by which the DPO is bound, there must be professional secrecy and confidentiality obligations shall apply while DPO is performing his functions, subject to any applicable professional secrecy or confidentiality laws.

COMPLAINTS PROCEDURE

Individuals may file a complaint with CHRISTABEL regarding compliance with the CHRISTABEL Privacy Policy or violation of their rights in accordance with the complaints procedure set forth in the relevant privacy commitment/policy or contract. Any request, complaint or claim of an individual involving the CHRISTABEL Privacy Policy will be evaluated against this Policy.

The complaint will be forwarded and managed by our accountable executive in cooperation with the directors of CHRISTABEL and our legal consultants when necessary.

REPLY TO INDIVIDUAL

Within one month of CHRISTABEL receiving a complaint, the individual shall be informed in writing of CHRISTABEL's position with regards to the complaint and/or of any action CHRISTABEL has taken in response to the complaint.

ADMINISTRATIVE FINES AND PENALTIES

Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

BASED ON THE ABOVE, the Personal Data Law established several criminal offenses punishable by a fine of up to:

EUR30,000 or up to three years' imprisonment or both for a breach of Section 33(1)(a) to (l) (Section 33(2), Personal Data Law).

• EUR10,000 or up to one years' imprisonment or both for a breach of Section 33(1)(m) and (n) (Section 33(3), Personal Data Law).

• EUR50,000 or up to five years' imprisonment or both for a breach of Section 33(1)(g) to (j), where the offense hinders the interests of the State or the operation of Government or threatens security (Section 33(4), Personal Data Law).

COOKIES

Stored cookies allow Christabel website to be more user-friendly and efficient for clients by allowing the Company to learn what information is more valued by clients versus what it is not.

The law states that we can store cookies on your device if they are strictly necessary for the operation of this site. For all other types of cookies, we need your permission.

For more information on the type of cookies we use kindly refer to the cookies policy attached hereto as **Appendix F.**

CHANGES TO THE PRIVACY POLICY

All versions of this policy will be shared and handed to all departments and employees of CHRISTABEL.

Any changes to the CHRISTABEL Privacy Policy require the prior approval of the directors CHRISTABEL companies.

Our Company keeps its privacy policy under regular review and places any updates on this web page.

This privacy policy was last updated on 11/07/2022.

APPENDIX A

Parental authorisation form

for processing the personal data of the minor (under the age of 14)

Dear parent/carer,

With the recent adoption of the General Data Protection Regulation (GDPR), the European Union (EU) assigned a prominent role to parental consent in order to protect the personal data of minors.

In Christabel Corporate Services Limited ("Christabel"), we only collect personal data of your children in the below situations:

a) When the minor is the registered Ultimate Beneficial Owner of a company;
b) When a service offered by Christabel is requested by you, on behalf of the minor (including but not limited to Migration Permits, land registry procedures, trust arrangements etc);
When this is requested by external third party advisors/service providers and or suppliers for the fulfilment of a contractual or legal/regulatory obligations i.e. immigration department.

The data of the minor shall be treated in accordance with the GDPR Legislation and in the manner described to you under the attached Privacy Notice.

To be completed by the parent / guardian / person with parental responsibility:

Full name of minor: ……..

Full name of parent / guardian completing this form: ……..

Relationship to the minor: ……

I acknowledge and confirm that I have read and understood Christabel's Data protection notice regarding the processing of the minor's personal data, and I hereby consent to have Christabel process the personal information provided for the purposes and to the extent stated therein.

I am aware that I reserve the right to withdraw this consent at any time.

Signature of parent of / guardian of /person who has parental responsibility:

_____

Name:
Date:

APPENDIX B

EMPLOYEES CONSENT FOR THE PROCESSING OF THEIR PERSONAL DATA

The Company only processes your personal data for the below purposes:

- Payroll
- Third party advisors (accountants, auditors, legal advisors)
- Processing of information for compliance purposes
- Processing of information for management purposes

CCTV- use of Surveillance equipment

I agree with the use of surveillance equipment in the workplace of the Company, which shall be solely used for the purposes of ensuring the security of Employer assets, and resident and employee safety. Surveillance equipment shall not be used for the purpose of regular monitoring of employees in the workplace.

Employee declaration

- ✓ I am giving my consent to the Company to use my data as indicated above
- ✓ I understand the ways in which the Company wishes to use my data as set out above
- ✓ I know that I can withdraw my consent at any time.
- ✓ If completed and signed electronically your digital signature will be legally binding

Name: ……...

Signed: ……

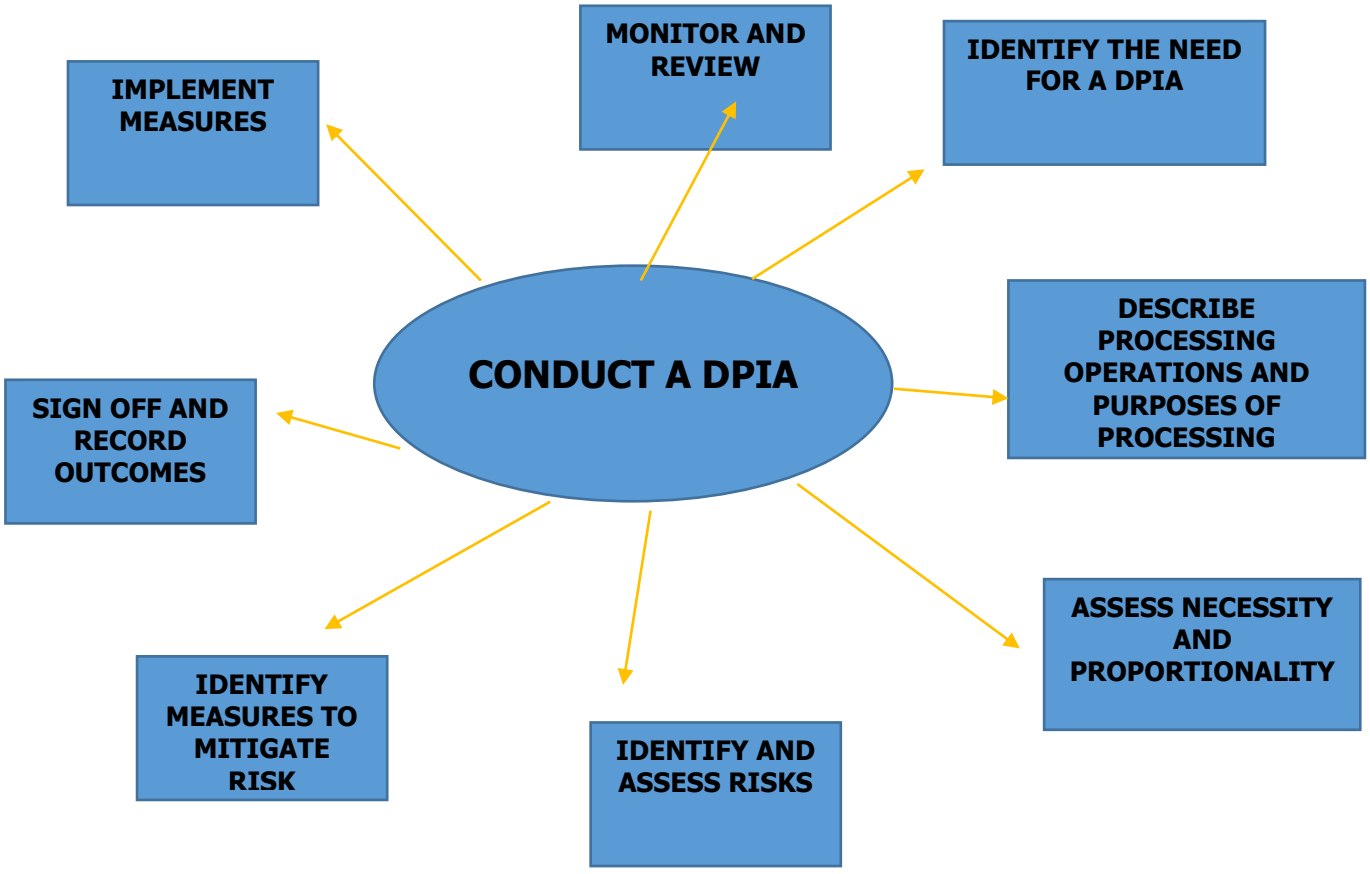
Date: ……..

APPENDIX C

DATA PROTECTION IMPACT ASSESSMENT

- We consider carrying out a DPIA in any major project involving the use of personal data.
- We consider whether to do a DPIA if we plan to carry out any other:
- evaluation or scoring;
- automated decision-making with significant effects;
- systematic monitoring;
- processing of sensitive data or data of a highly personal nature;
- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- innovative technological or organisational solutions;
- processing that involves preventing data subjects from exercising a right or using a service or contract.
- We always carry out a DPIA if we plan to:
- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- process special-category data or criminal-offence data on a large scale;
- systematically monitor a publicly accessible place on a large scale;
- use innovative technology in combination with any of the criteria in the European guidelines;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- carry out profiling on a large scale;
- process biometric or genetic data in combination with any of the criteria in the European guidelines;
- combine, compare or match data from multiple sources;
- process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- process personal data that could result in a risk of physical harm in the event of a security breach.
- We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- If we decide not to carry out a DPIA, we document our reasons.



APPENDIX D

INTERNAL REPORTING FOR DATA SECURITY BREACH

We are writing to inform you of a recent security incident at [name of company/organization]. This notification is sent pursuant to Article 33 of the General Data Protection Act

[Describe what happened in general terms including the date of the security incident, specific categories of personal/
private information that were involved, what you are doing in response and inform the letter's recipient as to what
they can do to protect themselves as indicated below.)

i.e On ___2022, we have discovered a data breach in our systems. The Data accessed may have included the following types of personal information:

Identity types of personal information breached: Email, First name, Last name

What Are We Doing?

Our platform provider has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information.

For More Information

If there is anything else that we can do to assist you, please contact +357 25 822766 weekdays between the hours of 8.30am and 6pm.

APPENDIX E

PRIVACY NOTICE

The present Privacy Notice is prepared in the light of the **General Data Protection Regulation (EU Regulation 2016/679)**, hereinafter "GDPR" and "the Regulation" respectively, which is applicable as of the 25th of May 2018.

"Personal Data" means any information relating to an identifiable person (natural person) who can be directly or indirectly identified.

"Processing" means various types of operations regarding the Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Responsibility for Processing of Personal Data

"Controller" of your personal data is Christabel Corporate Services Limited, an Administration Service Provider registered under the laws of the Republic of Cyprus, with registration number HE205472, with registered office address at 118 Agias Fylaxeos, Christabel House, 3087 Limassol, Cyprus. References to the Controller in this Privacy Policy include:

- Christabel Support Services Limited, with principle place of management at 118 Agias Fylaxeos, Christabel House, 3087 Limassol, Cyprus, arranging the accounting and bookkeeping on behalf of customers.
- Highsight Rentals Ltd, with principle place of management at 10 Pikionis, 3075 Limassol, Cyprus, providing services of office rentals.

The Controller collects and/or processes the Personal Data of existing, future and former clients. The term clients may include individuals to whom a service is provided directly and/or individuals who act as signatories on behalf of the individual, contact persons, attorneys and/or officers, directors, shareholders and ultimate beneficial owners in case of Corporate clients.

The Controller collects and processes the Personal Data of an Individual on a lawful basis in order to comply with other Law and Directives related to the services provided, (Article 6(1)(c) of the Regulation).

The type of Personal Data the Controller may collect is:

Demographic Data	Name, Gender, Date of Birth, Age, Nationality, Citizenship
Contact Details	Home/Work Postal Address, Home/Work landline phone number, Home/Work mobile phone number, Personal/Work email address
Financial Data	Source of Funds and Source of Wealth, information on financial transactions (where applicable), Tax Residency information, Tax Declaration
Personal and Professional Data	Information on education, employment and family of the individual and information on any potential political involvement of the individual
Correspondence Data	Records of any Correspondence with the individual

How the Personal Data is collected:

- directly from you;
- your authorised representatives;
- business introducers;
- publicly available sources;
- government and law enforcement agencies;
- generated by ourselves.

How this information is used

The Controller evaluates your Personal Data both manually and automatically to evaluate certain personal aspects, hereinafter referred to as **"profiling"**.

The Controller is legally obliged to take anti-money laundering, anti-fraud and anti-terrorist financing measures. Data evaluations are also carried out in this context. Each element of the information collected from the individual is being scored in order to evaluate the risk each individual bears.

With whom your Personal Data are shared

The Controller keeps your Personal Data safe and provides access to the officers of the Controller who require such access to perform their tasks and to facilitate your requests.

The Controller, may share your information with third parties in order to provide services to you. Those third parties may include:

- banks, financial institutions and any other similar organizations that are nominated by the Client;
- auditors;
- accountants;
- agents;
- lawyers/advisors;
- to Companies providing services such as packaging, mailing and delivery purchases, postal mail etc;
- any organization at the Client's request or any person acting on behalf of the client;
- any third parties where this is necessary to process a transaction or provide services which the client has requested.

The Controller may be required by law or regulation or court order to disclose your Personal Data to Governmental, legal, regulatory or similar authorities, central and/or local government agencies, any tax authorities and the police.

International Transfer of Personal Data

Your Personal Data may be transferred outside of the European Economic Area ("EEA") when this is required for: the execution of your orders or where it is prescribed by the law and/or under your consent.

Whenever the Controller sends your Personal Data outside the EEA, the Controller will make sure that your Personal Data is protected in the same way as if it was being used in the EEA. The Controller will use one of the following safeguards:

- Adequacy Decision of the European Commission;
- Suitable Standard Contractual Clauses to ensure equivalent protection to the EEA; or
- Other valid transfer mechanisms.

Data Security of your Personal Data

The Controller commits to ensure protection of your Personal Data by applying appropriate technical and organisational security measures to ensure protection of your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access.

You are responsible for ensuring that any Personal Data send to the Controller are send securely.

In instances where the Controller discloses your Personal Data to third parties, within EEA, requires such third parties to have appropriate technical and organization measures to ensure the protection of your Personal Data.

Data Storage

The Controller will keep your information for as long as you have a relationship with us. After the end of the business relationship, the Personal Data will be kept for the period of at least five years in order to meet any legal, accounting or reporting obligations.

YOUR Legal Data Protection Rights

The Regulation provides you with several rights regarding your Personal Data. A summary of those rights is given here below. For more complete information please refer to the Regulation Articles 15 to 21.

- **Right of Access;** access your Data from the Controller and confirm whether or not they are being processed, *(see Article 15 of the Regulation)*.
- **Right to Rectification;** correct inaccurate Personal Data we hold about you, *(see Article 16 of the Regulation)*.
- **Right to be Forgotten;** entitles you to submit a request to the Controller to delete or remove your personal data, in certain cases, as there is no longer necessity and/or you have withdrawn your consent and/or you have objected to the processing etc *(see Article 17 of the Regulation)*. The Controller may have legal or other official reasons that needs to keep your Personal Data.
- **Right to Object;** you have the right to object to the processing of your Personal Data in certain cases, *(see Article 21 of the Regulation)*.
- **Right to Restrict;** enables to you suspend the processing of your Personal Data in certain cases, *(see Article 18 of the Regulation)*.
- **Right to data Portability;** request the transfer of your Personal Data to you or to a third party, *(see Article 20 of the Regulation).*
- **Right to file a complaint;** if you are unhappy with the use of your Personal Data by the Controller, you have the right to file a complaint with the supervisory authority.

Procedure on filing a complaint

You have the right to lodge a complaint with the Commissioner, if you consider that the processing of personal data relating to you infringes the GDPR.
Prior to lodging your complaint, you may contact directly the DPO at privacy@christabelonline.com to address your concerns.

Lodging a complaint with the Commissioner

For lodging a complaint you are requested to fill in one of the following forms, depending on the case, and send it to the Commissioner:

Form A: Complaint involving the data subject's rights (right of access, right to object or to rectification or to erasure or to the restriction of processing or to data portability).
Form B: Complaint involving any other breach of the legislation for the processing of personal data (other than the rights).
Form C: Complaint concerning unsolicited electronic communication i.e. emails and sms (spam).

All of the above mentioned forms can be found through the Office of the Commissioner for Personal Data Protection Website as seen below:
(http://www.dataprotection.gov.cy)

Once the authority investigates the complaint, it will contact you to inform you of the results of the investigation

Complaints which are ambiguous, excessive, particularly, or if they are anonymous or do not contain the necessary details, may not be examined. In such case the complainant shall be duly informed.

Penalties imposed when lodging a complaint

In cases where the controller and/or processor are found to be in breach of the data protection legislation, the Commissioner may impose corrective measures (including fines). The case may also be referred to the Police by the Commissioner. The Commissioner can notify to the Attorney General of the Republic and/ or to the police any violation of the provisions of the Regulation or of the law 125(me) /2018 that may constitute an offense.

Withdraw of Consent

Where the Controller relies on your consent for the processing of your Personal Data, you may withdraw your consent at any time by sending us an email at privacy@christabelonline.com. The Controller shall inform you before giving effect to your withdrawal notification.

Changes to this Privacy Notice

The Controller may amend this privacy notice from time to time. A copy of the latest version of this notice will be available from our Website and will be provided to you upon request. In case of significant changes, the Controller will bring this changes to your attention.

For any matters related to the Data Protection please contact the Data Protection Officer at privacy@christabelonline.com.

☐ I have read the Privacy Notice and I Consent to its context
☐ I have read the Privacy Notice and I DO NOT Consent to its context

Name Signature

APPENDIX F

COOKIES POLICY

Directive 2009/136/EC:

The European Parliament directed that all countries within the EU must set up laws requiring websites to obtain informed consent before they can store or retrieve information on a visitor's computer or web-enabled device.

1. You need to provide detailed information regarding **how** that cookie data will be utilized.
2. You need to provide visitors with some means of **accepting or refusing** the use of cookies in your site.
3. If they refuse, you need to ensure that cookies will not be placed on their machine

Exception for cookies that are "strictly necessary" to fulfil the services requested by your site visitors.

Necessary

These cookies are necessary to make the website usable, allowing basic functions, such as navigation and access to secure areas of the website. You can only disable them through your browser settings, but this may affect the proper functioning of the website.

Analytics cookies

We use these purely for internal research on how we can improve the service we provide for all our users.
The cookies simply assess how you interact with our website — as an anonymous user (the data gathered does not identify you personally).
Also, this data is not shared with any third parties or used for any other purpose.

Marketing (Advertising)

Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third party advertisers.

Preference cookies

Enable a website to remember information that changes the way the website behaves or looks, like your preferred language or the region that you are in.