Personal Data Protection (Privacy) Policy

Last review: January 2024

CONTENTS

PREAMBLE

DYNGROUP LTD, a company incorporated and registered in Cyprus with registration number HE402426 whose registered office is at Gianni Gkoura 3, FRIENDS BLOCK B, Flat/Office 201, Germasogeia, 4040 Limassol Cyprus ("DYNGROUP" or "We").

The business of the Company is subject to the requirements of regulations and rules which regulate the personal data protection of the Company`s clients. The Company has developed this Personal Data Protection (Praivicy) Policy (hereinafter the "Policy") to meet all the requirements of Cyprus and EU legislation and the best international standards in the field of data protection and confidentiality.

DEFENITIONS

- Personal Data Protection Legislation means:
  i. Cyprus Data Protection Act (2018) ;
  ii. General Data Protection Regulation (GDPR) of the dated 25 May 2018 (the "data protection legislation") governs the processing of personal data (EU Regulation (EU) 2016/679).

  The data protection legislation requires that personal data including special categories of personal data, which are regarded as more sensitive, must be processed by data controllers in accordance with the data protection principles set out in the GDPR.
- Data controller - a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Company is a data controller for the purposes of data protection legislation.
- Data processor - any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
- Data subject - any natural person who is the subject of personal data.
- Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.
- Special categories of personal data – personal data revealing 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 person, data concerning health or data concerning a natural person's sex life or sexual orientation. Information about the commission of offences or criminal proceedings is also regarded as sensitive under data protection legislation and we handle such information commensurately.
- Transfer of data outside the Company – when data is transmitted, sent, viewed or accessed in or to a country outside the Company.
- Personal data - means any information relating to an identified or identifiable natural person (the "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

  The above definition includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

I. PERSONAL DATA PROTECTION (PRAIVICY) POLICY

1. Policy statement

1.1. Data Protection Policy sets out how the Company intends to comply with data protection legislation and will handle personal data (and other sensitive information) in a way which will help us effectively to discharge our functions in the public interest, uphold clients' and the public's confidence in us as a service provider, and ensure that we are a fair and effective Company.

2. Policy goals

2.1. This Policy aims:

(a) to state our commitment to compliance with data protection legislation and the principles of data

protection;

(b) to discharge Company`s obligations to have in place data protection policies as part of measures to secure compliance with data protection legislation;

(c) to provide a general appropriate Policy document and an overarching appropriate Policy document for processing of special categories of personal data, as may be required as part of data protection legislation;

(d) to outline how we will work to comply with the data protection legislation through the use of technical and organisational measures and in particular the principles of data protection by design and data protection by default;

(e) to state the responsibility of everyone working for us or on our behalf to comply with this Policy and the data protection legislation;

(f) to identify some of the circumstances where we are exempt from certain general principles because of our functions as a regulator.

3. Scope

3.1. This Policy applies to all personal data as defined by the data protection legislation whether it is held by us, transferred to or exchanged with third parties, or held by third parties on behalf of us. This applies whether the data is held in electronic and paper form.

4. Roles and responsibilities

4.1. The Compliance officer is ultimately responsible for the Company`s compliance with data protection legislation.

4.2. The Chief Executive Officer is responsible for maintaining of this Policy.

4.3. The Compliance Officer has the responsibilities set out in the General Data Protection Regulation.

4.4. Managers are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties.

4.5. Managers must contact the Compliance officer if they are unsure about what security or other measures, they need to implement to protect personal data.

4.6. Managers must always contact the Compliance officer if:

(a) they are unsure of the lawful basis which they are relying on to process personal data;

(b) they need to rely on consent for processing personal data;

(c) they need to prepare privacy notices or other transparency information;

(d) they are unsure about the retention period;

(e) they are unsure on what basis to transfer personal data outside the Cyprus;

(f) they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment[1];

(g) they plan to use personal data for purposes other than those for which it was originally collected;

(h) they plan to carry out activities involving automated processing including profiling or automated decision-making;

(i) they need help with any contracts or other areas in relation to sharing personal data with third parties (including the Company's contractors);

(j) they plan to share data with another organisation or person in a way which is new or could affect data subjects' rights.

4.7. Everyone working for the Company is responsible for ensuring that they understand and follow this Policy and other procedures relating to the processing and use of personal data and support the Company in complying with data protection legislation.

5. Compliance

[1] Art. 35 GDPR

5.1. Everyone working for the Company or on the Company`s behalf is required to comply with this Policy.

5.2. Staff will be required to complete mandatory data protection training.

5.3. The Company will regularly review the systems and processes under its control to ensure they comply with this Policy.

5.4. The Company will investigate any alleged breach of this Policy. An investigation could result in the Company's taking action up to and including dismissal; removal from office; or, termination of a contract for services.

6. Policy review

6.1. The Company will review this Policy every year or more frequently in the event of any legislative or regulatory changes.

7. The data protection principles

7.1. The principles set out in data protection legislation require personal data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency);

(b) Collected only for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (Purpose limitation);

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data minimisation);

(d) Accurate and where necessary kept up to date (Accuracy);

(e) Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation);

(f) Processed in a way that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality);

(g) Not transferred to another country without appropriate safeguards being in place (Transfer limitation);

(h) Made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (data subject's rights and requests).

(i) Company`s Mobile App/Website/Service is not intended for use by children. We do not knowingly collect personal information, including any personal data, from children. If you are a parent or guardian and believe your child has provided us with their personal data, please contact us immediately.

7.2. The Company is responsible for, and must be able to demonstrate compliance with, the data protection principles listed above (Accountability). This Policy sets out below, in general terms, how the Company approaches these matters.

8. Processing and use of personal data

8.1. The Company will maintain a general record of processing which sets how we process personal data in accordance with data protection legislation. Such records imply the login of all actions with personal data, indicating the reasons for their processing, the persons involved in the processing, the date of processing and the result of processing personal data.

8.2. In general terms, we primarily process personal data about:

(a) People working for the Company or on behalf of the Company;

(b) People helping the Company to perform its regulatory functions;

(c) Clients' identification data in accordance with AML, CTF procedure as set in the respective Policies;

(d) External stakeholders and customers engaging with the Company about the work we do, including those who wish to make a complaint about us.

8.3. The Company does not generally rely on consent to process personal data and special category personal data as set in para 8.4 below.

8.4. The Company generally relies on the following lawful bases for processing personal data:

(a) the processing is necessary to perform a contract with the data subject;

(b) the processing is necessary to comply with the relevant legal obligations;

(c) the processing is necessary to perform a task carried out in the public interest or in the exercise of official authority request.

8.5. Certain activities we carry out may not be covered by the above. In such circumstances, the Company will record the legal basis for processing.

8.6. The Company processes certain special category of personal data in connection with its functions as an employer and to perform certain regulatory obligations. For example, we investigate allegations relating to health or cautions and convictions. In general terms, the legal bases for such processing are:

(a) It is necessary for the purposes of performing or exercising obligations or rights of the Company or the data subject for the purposes of employment;

(b) It is necessary for the exercise functions as set out in the special legislation and is necessary for reasons of substantial public interest;

(c) It is necessary for the purposes of promoting and maintaining equality of opportunity or treatment by the Company;

(d) It is necessary for preventing or detecting unlawful acts, must be carried out without the consent of the data subject so as not to prejudice those purposes, and is necessary for reasons of substantial public interest;

(e) It is necessary to protect the public against dishonesty, malpractice, unfitness or incompetence, must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and is necessary for reasons of substantial public interest.

8.7. If any data subject has reason to believe that applicable law does not allow DYNGROUP to fulfil its obligations under this Policy, they shall immediately inform the person responsible for the protection of personal data at DYNGROUP by sending a request to the following email address: dyngrouplegal@gmail.com

9. Transparency

9.1. General information about how the Company process personal data of its clients (if any) as a data controller (referred to as "fair processing information")[2] will be available on the Company's website through privacy notices and other public-facing material.

9.2. As a data controller, the Company is excluded from certain obligations to provide fair processing information (and other data subject rights) if the processing would prejudice the proper exercise of its functions. Similarly, the Company may not make fair processing information available where personal data is processed to get legal advice, for the purpose of legal proceedings (including prospective legal proceedings), or to share information with the police, exchanges regulatory bodies or other law enforcement bodies[3].

10. Purpose limitation

10.1. The Company ensures that all collected data is only for specified, explicit and legitimate purposes. The Company will not go on to process data in any way that is incompatible with the original purposes.

10.2. Where the Company intends to use data for a different or incompatible purpose from that relied upon when it first obtained it will:

(a) have an appropriate legal basis for the new purpose;
(b) assess the privacy implications of the proposals;
(c) inform the data subject of the new purpose and the legal basis for processing.

10.3. Information we may collect and how we use it

№	Categories of personal information collected	Categories of sources from which personal information is collected	Business or commercial purposes for collection, use, and sharing	Categories of third parties with whom some or all of the personal may be shared

[2] Art. 5-6, GDPR

[3] Art. 31, GDPR

1.	Personal and online identifiers (such as first and last name, email address, phone number, usernames, or unique online identifiers)	Directly from you Marketing partners	To provide and Improve the Services Personalization of the Services Customer support Marketing and targeted advertising Security and fraud prevention	Customer service partners Marketing sponsors and partners Ad networks E-Commerce vendors Endeavor Analytics services
2.	Financial Account Information (such as credit card numbers, bank account information, Paypal account information)	Directly from you Payment providers E-Commerce vendors	To provide the Services	E-Commerce vendors Payment providers Fraud and cybersecurity companies Endeavor
3.	Government IDs (such as passport or TAX ID)	Directly from you	To provide investment related services	Endeavor Directly managed E-tols providers
4.	Customer Profile Information (such as race, gender, age range, income range, ad demographics)	Directly from you Marketing partners Ad networks Third party data providers	To provide and improve the Services Personalization of the Services Direct marketing Targeted advertising Analytics Research and development Security and fraud prevention	Endeavor Analytics services Ad networks Technology service providers Marketing sponsors and partners
5.	Transactional Information	Directly from you E-Commerce vendors	To Provide and Improve the Services Customer Support Analytics Research and Development	Endeavor Analytics services Technology service providers E-Commerce Vendors
6.	Communications with you (such as customer support messages, emails, social media posts)	Directly from You Customer support partners	To Provide and Improve the Services Customer Support	Endeavor Analytics services Technology service Providers E-Commerce vendors Customer Service Partners
7.	Non-Precise Geolocation information (such as zip or	Directly from you	To provide and improve	Endeavor

	area code, state, country)	Cookies and similar technologies Marketing sponsors Technology service providers Ad networks	the Services to you Personalization of the Services Fraud and cybersecurity Direct marketing Targeted advertising	Ad networks Technology service providers Marketing sponsors
8.	Precise Geolocation (such as full address or specific location while at an event)	Directly from you Marketing Sponsors Technology service providers	To provide and improve the Services to you Personalization of the Services Direct Marketing	Endeavor Ad Networks Technology service providers Marketing sponsors
9.	Other information about you that is linked to the personal information above	Directly from you Endeavor Third party data providers Marketing sponsors.	To Provide and Improve the Services Personalization of the Services	Endeavor Ad networks Marketing sponsors
10.				

11. Use of “cookies” files

11.1 When using the Website/Mobile application, cookies are used, which are installed on the Users' electronic devices. DYNGROUP uses the following categories of cookies:

- ✓ to provide Users with stable access to the functionality of the Website;
- ✓ to improve and facilitate the use of the Website/Mobile Application by Users;
- ✓ for the correct display of DYNGROUP advertising messages within the Website;
- ✓ to provide access to Users to exchange information from the Website/ through social networks;
- ✓ to research indicators related to the audience of the Website (traffic analysis, usage trends).

11.2 DYNGROUP requests the Users' consent to the use of "cookies" files before starting to use the Website by sending a corresponding electronic message (in the form of a banner).

Users have the following options regarding cookies:

- ✓ allow automatic saving and use of "cookies" files;
- ✓ warn about the use of "cookies" files;
- ✓ always block the use of "cookies" files (possible restrictions on the use of the Website in

the form of the impossibility of setting individual settings by users).

11.3. The use of the Website/Mobile application involves the use of the functionality of other resources, including:

- ✓ social networks (on the Website/Mobile Application there is an option for the user to distribute content directly from the Website) (depending on the functionality and internal settings of the Website/Mobile Application). The procedure for using "cookies" files is regulated by the relevant policies of such companies;

- ✓ Google Analytics to collect general statistical information about the use of the Website/Mobile Applications (such information is used by the Company exclusively to improve the content and services for the use of the Website/Mobile Application). The procedure for functioning of Google Analytics is governed by the relevant company policy;

- ✓ other resources, the safe use of which has been verified by DYNGROUP.

11.4. DYNGROUP draws attention to the fact that blocking the use of "cookies" files may lead to incorrect functioning of the Website. Users have the right to block the use of cookies in whole or in part (certain types of cookies) by making changes to the web browser settings of the devices they use to access the Website.

12. Use of geolocation data

12.1. When you use our Mobile App/Website/Service, we may collect the following types of geolocation data:

- ✓ GPS-based location information.

- ✓ IP address and other device identifiers that may provide approximate location data.

- ✓ Wi-Fi access points and cell towers near your device that may provide approximate location information.

- ✓ Other location-based information provided by you or your device.

12.2 We use geolocation data for the following purposes:

- ✓ To provide location-based services, such as finding nearby points of interest or delivering location-specific content.

- ✓ To improve our [Mobile App/Website/Service] and optimize user experience based on location.

- ✓ To analyze user trends and behavior to enhance our services and tailor content.

- ✓ To personalize your experience, such as providing relevant advertisements and recommendations based on your location.

- ✓ To comply with legal and regulatory requirements.

12.3. We may share your geolocation data with third parties in the following circumstances:

- ✓ With service providers and partners who assist us in providing location-based services and enhancing our [Mobile App/Website/Service].

- ✓ With advertisers and marketing partners to deliver targeted advertisements based on your location.

- ✓ With law enforcement agencies or authorities if required by law or to protect our rights and safety.

- ✓ In the event of a merger, acquisition, or sale of all or a portion of our assets, your geolocation data may be transferred to the acquiring entity.

12.4. We employ industry-standard security measures to protect your geolocation data from unauthorized access, disclosure, or alteration. However, no data transmission over the internet or method of electronic storage is 100% secure. Therefore, while we strive to use commercially acceptable means to protect your data, we cannot guarantee absolute security.

12.5. You have the right to control how your geolocation data is collected and used. You can disable location services on your device or adjust app settings to restrict location access. However, disabling location services may limit certain features and functionalities of our Mobile App/Website/Service.

13. Data minimisation

13.1. The Company will process personal data in a way that is adequate, relevant and limited to what is necessary for its purposes.

13.2. All personal data must be handled through corporate computer systems with the relevant security level according to the Company`s respective Policy.

13.3. Unnecessary copies of information must be deleted or securely destroyed.

13.4. Staff and contractors must only process personal data as required to carry out their role. The Company may monitor or audit the use of data to ensure that this happens.

14. Accuracy

14.1. The Company ensures as far as possible that the data the Company holds is accurate and kept up to date. In some circumstances the Company may need to keep factually inaccurate information or an opinion which someone agrees with as part of its regulatory functions, such as where the Company investigating an allegation that a person's entry on our register has been incorrectly obtained or fraudulently procured.

14.2. Staff and contractors are responsible for checking the accuracy of any personal data the Company collects. Staff and contractors must take all reasonable steps to destroy or update inaccurate personal data.

15. Storage limitation, retention and destruction

15.1. The Company ensures that personal data is not kept in an identifiable form for longer than is necessary and in general if there no exemption prescribed by the relevant legislations personal data storage period shall not exceed 90 calendar days.

15.2. Because of functions as a security dealer, the Company keeps some personal data for long periods of time as prescribed by the various data-storage regulations and procedures.

15.3. Staff and contractors are responsible for storing personal data in accordance with this Policy and complying with the retention periods set out in special regulations.

15.4. In any case, if there are no special judicial or legislative regulations, personal data cannot be stored for more than 10 years and upon expiration of this period are subject to immediate removal.

16. Security, integrity and confidentiality

16.1. The Company develops, implements and maintains appropriate data security systems to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

16.2. The Company will regularly review, evaluate and test the effectiveness of its data security systems (at least

annually).

16.3. Staff and contractors must comply with this Policy. These policies set out the actions that must be taken to protect the 'Confidentiality', 'Integrity' and 'Availability' of all personal data from the point of collection to the point of destruction. In this context:

(a) 'Confidentiality' means only people who are authorised to know and use personal data can access it;
(b) 'Integrity' means that personal data is accurate and suitable for the purpose for which it is processed; and
(c) 'Availability' means that only authorised peoples are able to access the personal data when they need it for authorised purposes.

17. Security incidents

17.1. Anyone involved in or witness to an information security incident (or suspected incident) must inform the Company`s Compliance officer of the incident as soon as possible after its occurrence at dyngrouplegal@gmail.com

17.2. Information security incidents must be reported and managed in accordance with the Information Technology Security Policy.

18. Transfer limitation

18.1. The Company should normally only transfer data outside where it is:

(a) necessary to fulfil its functions as a data controller;
(b) necessary in the public interest (for instance, to fulfil the functions of a similar data controller overseas, only with the previous confirmation from special state authority if such confirmation is required)[4]
(c) the data subject has explicitly consented to the transfer; or
(d) necessary to issue or defend legal claims according to legislative procedure.

19. Rights and requests

19.1. Data subjects wishing to exercise their rights under data protection legislation should generally make their request in writing via the Company's website or by letter to the relevant email: dyngrouplegal@gmail.com so that the request can be processed by the Company.

19.2. Any member of staff or contractor who receives a request from a data subject to exercise their rights must pass the request on to the Company's responsible officials as soon as possible.

20. Record keeping

20.1. All staff and contractors must keep and maintain accurate corporate records reflecting data processing.

21. Privacy by design (where applicable)

21.1. The Company implements appropriate technical and organisational solutions (like pseudonymisation[5]) to ensure compliance with data privacy by design principles.

21.2. Managers are responsible for assessing and implementing appropriate privacy by design solutions on all programmes, systems and operations that involve processing personal data. In doing so managers will take into account the following:

(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of processing; and
(d) any adverse impact the processing may have on the rights and freedoms of data subjects.

22. Data protection impact assessments

[4] Art. 49, GDPR
[5] Art. 29, GDPR

22.1. The Company considers the need for, and where appropriate goes on to conduct, with Data Protection Impact Assessments (DPIAs) in respect of our data processing activities according to the Company`s Information Technology Security Policy.

22.2. The Company will conduct a DPIA where it undertakes a new processing activity which is likely to result in a high risk to the rights and freedoms of the data subject.

22.3. In particular, Directors will ensure a DPIA is carried out when proposing major system or business change programmes, or conducting reviews of such programmes, which involve the:

(a) Use of new or changing technologies (programs, systems or processes);
(b) Automated processing including profiling and automated decision making;
(c) Large scale processing of special category or other sensitive personal data; and
(d) Large scale, systematic monitoring of a publicly accessible area.

23. Automated processing and decision making

23.1. Generally, the Company is engaged in automated processing/profiling, or automated decision-making.

23.2. Where the Company engages in an automated decision making/profiling, we will inform the data subject of the reasons for the decision making or profiling and any consequences arising. The Company also will give to the data subject the right to request human intervention, express their point of view or challenge the decision. Where possible the Company will do this prior to the decision being taken.

24. Data processors

24.1. The Company may contract with other organisations to process personal data on its behalf.

24.2. The Company will only appoint a data processor if, having carried out due diligence, it is satisfied that they can implement appropriate technical and organisational measures that meet the requirements of the data protection legislation.

24.3. The appointment of a data processor must include the contractual requirements specified in the data protection legislation.

24.4. The Compliance Officer may be asked to advise on contractual arrangements with data processors.

25. Data sharing

25.1. Any sharing of personal data with external third parties without previous approval by the data subject is prohibited except for the case of special legislative prescriptions. In any case all such data sharing must comply with this Policy, as relevant.

26. Complaints procedure

26.1. Anyone who considers that this Policy has not been followed may make a complaint following the Company`s complaints procedure. The complaint will be reported to the Internal Audit who may be asked to advise on the response or via whistleblowing system. Internal Audit may investigate the matter itself or direct to the Company's Compliance Officer.

26.2. If, after checking the appeal regarding non-compliance with certain provisions of this Policy, the Compliance officer of the Company will find out that violations have occurred, the Compliance officer performs the following actions:

(1) Identifies what specific Policy provisions were violated and what was the substance of the violation.

(2) Establishes those responsible for non-compliance with the Policy provisions.

(3) Presents the results of the investigation to the CEO and the Board of Directors with recommendations regarding disciplinary responsibility of the persons who committed the violation (if such measures are necessary) and/or amending the Company's Policy and/or software and hardware to minimize and prevent identified violations in the future.

(4) Notifies interested parties of identified violations of policies and measures taken by the Company to eliminate and prevent them in the future.

26.3. The Board of Directors of the Company, as a result of the investigation, would take the following decisions:

(1) Brings to disciplinary responsibility the persons who have committed non-compliance or violation of the requirements of this Policy (if it considers such measures appropriate) and relevant legislation if

applicable.

(2) Initiates changes to the existing rules and procedures of this Policy and/or software and hardware to minimize and prevent detected violations in the future.

(3) Considers the issue of compensation for damage to third parties, if such is demanded and was caused by a violation of this Policy and relevant legislation if applicable.

VALIDITY DATE AND PERIODIC REVIEW

This Policy is effective on the Company's wide basis from the date of its publication.

Its contents will be reviewed periodically, and any changes or modifications will be made as appropriate.

VERSION CONTROL TABLE

Version	Approval Date	Changes Description	Management Board member's signature confirming approval
1.1	12.01.2024		