Data Protection Policy

DIMAND Group of Companies

Version:	**2.0**
CEO's Approval Date:	**20/06/2024**

Table of Contents

1. Applicable legislative and regulatory framework

The European Parliament and the Council of the European Union have issued Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "General Data Protection Regulation" / GDPR)

This Regulation which entered into application on 25 May 2018 establishes a unified regulatory and legal framework on the protection of personal data in all European Union member states. Furthermore, to facilitate the implementation of GDPR into the Greek legal system, L.4624/2019 was adopted, which includes additional cases of personal data processing and expands on other subsectors of data protection.

2. Company and Group of Companies Commitment to GDPR and L.4624/2019 Compliance

Within this framework, ensuring data protection and compliance with GDPR and L. 4624/2019 is a top priority for the Parent Company of the "**DIMAND SOCIETE ANONYME - DEVELOPMENT AND EXPLOITATION OF REAL ESTATE AND CONSTRUCTIONS, SERVICES AND HOLDING**" Group of Companies, trading as "**Dimand S.A.**" (hereinafter "the Group" or "DIMAND").

To this end, DIMAND Group of Companies has established and implements this Data Protection Policy (hereinafter "this Policy").

3. Purpose of this Policy

The purpose of this Policy is to protect individuals' personal data processed by DIMAND Group of Companies, thus affirming the Group's ultimate objective and commitment to uphold human rights and freedoms, including the right to privacy and personal data.

4. Scope of this Policy

This Policy applies to all personal data processing carried out by the Group or for a company within the Group, and pertains to all Company employees and any third-party associates (all suppliers, subcontractors, surveyors, external collaborators, advisors etc.) involved in the processing of personal data.

5. Definitions

The following table lists alphabetically the key terms used in this Policy, along with their respective definitions and meanings.

Term / Acronym	Definition
Recipient	The natural or legal person, public authority, agency or another body, to which the personal data is disclosed, whether a third party or not. However, public authorities to which personal data may be disclosed in the framework of a particular inquiry in accordance with Union or Member State law should not be regarded as recipients; the processing of this data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
GDPR	General Data Protection Regulation / Regulation (EU) 2016/679
Personal Data ('Data')	Any information concerning an identified or identifiable natural person ('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, psychological, genetic, mental, economic, cultural or social identity of that natural person;
Board of Directors (the 'Board')	The Board of Directors of the Group's Parent Company
Special categories of Personal Data ('sensitive data')	Personal data revealing: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • genetic data; • biometric data; • data concerning health; • data concerning a natural person's sex life, • or sexual orientation.
Processor	The natural or legal person, public authority, agency or another body which processes personal data on behalf of the Controller
Processing	Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as: • collection; • recording;

	• organization; • structuring; • storage; • adaptation; • alteration; • retrieval; • consultation; • use; • disclosure by transmission; • dissemination • or otherwise making available; • alignment; • combination; • restriction; • erasure; • destruction.
Supervisory Authority	The Hellenic Data Protection Authority ('HDPA')
Company	The company **"DIMAND SOCIETE ANONYME - DEVELOPMENT AND EXPLOITATION OF REAL ESTATE AND CONSTRUCTIONS, SERVICES AND HOLDING"**, trading as **"DIMAND S.A."** / the Parent Company of DIMAND Group of Companies
European Union	The twenty-seven (27) Member States of the European Union
European Economic Area	The twenty-seven (27) Member States of the European Union together with Norway, Iceland and Lichtenstein.
Group	The DIMAND Group of Companies
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements; Example: Profiling is the collection of data that includes information such as the data subject's social contacts, political and personal opinions, financial capacity, health condition and other information which is combined to provide a greater picture of the data subject.
Main establishment	The main establishment of a Controller is the place where the Controller makes key decisions as regards the purposes and the means of the processing of personal data.
Child	According to the GDPR, a child is any person under the age of 16 years. The processing of a child's personal data is lawful only if consent is granted by the parent or holder of parental responsibility over the child.

Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Consent of the Data Subject	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.
Filing System	Any structured set of personal data which is accessible according to the specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.
Third Party	Any natural or legal person, public authority, agency or body other than the data subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorized to process personal data.
Controller	The 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.
Data Subject	Any living individual to whom the personal data pertains.

Controller

6. Governance: Compliance with the GDPR and the relevant regulatory framework per role

Board of Directors (the 'Board')

The Company's Board of Directors plays a key role in ensuring the Company's compliance with the provisions of the GDPR. In this framework, the Board has the following non-exhaustive powers:

- **Raising awareness and training:** The Board is responsible for ensuring that company staff is well-informed and adequately trained as regards the GDPR's principles and requirements.
- **Strategy definition:** The Board shall establish and implement a clear GDPR compliance strategy, tailored to the Group's scale, structure and activities.
- **Inspection and assessment:** The Board shall set up mechanisms to regularly inspect and assess the efficacy of the GDPR compliance measures.
- **Handling breaches:** In the event of a data breach, the Board shall act swiftly and effectively to mitigate the incident and reduce any adverse effects.

Management

The CEO and the Senior Management of the Group's Parent Company shall be liable for implementing this Policy.

In addition, the above persons shall be liable for developing and encouraging sound personal data management practices throughout the Group.

Employees

Group employees shall ensure due processing of personal data under the Group's management as the Controller.

Third Parties (Processors)

Any third party acting as Processor on behalf of the Group's Parent Company is responsible for the processing of personal data, as set out in this Policy, and always in accordance with the instructions given by the Company.

7. General principles governing the processing of personal data

Any personal data processing within the Group shall be carried out in accordance with the personal data protection principles, as laid down in article 5 of the GDPR.

In particular, the principles are as follows:

A. Principle of lawfulness, fairness and transparency of data processing

Personal data is processed lawfully and in a transparent manner. Any natural person or legal entity processing personal data shall ensure their compliance with this Policy and the relevant applicable regulatory framework, such as the GDPR.

A.I. *Lawfulness*

Prior to the commencement of any personal data processing, the legal basis for such processing shall be acknowledged, i.e. the legitimate grounds. Consent, for example, is one of the legal bases for processing.

Where processing is based on consent given prior to any processing, the data subject shall be informed accordingly and shall grant their consent freely and in a clear and distinguishable manner. Consent may be granted both explicitly and implicitly, for example by providing personal data to the Controller. While consent is not required to be in written form, it is advisable to obtain written consent or authorized audio recording to facilitate verification (e.g. before courts and other authorities). The data subject shall have the right to withdraw their consent at any time; it shall be as easy to withdraw as to give consent.

Consent is not required in the following cases:

- processing is necessary for the performance of a contract to which the data subject is a party;
- processing is necessary for compliance with a legal obligation to which the

Controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company;
- processing is necessary for the purposes of the legitimate interests pursued by the Company, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
- where the data subject has granted public access to their personal data, for example by publishing it in newspapers or listing it in telephone directories, and such processing has not been forbidden by the data subject.

A.II Fairness

In order to ensure fairness in data processing, the Controller shall provide data subjects with specific clarifications, where available.

A.III Transparency

Adequate information regarding the personal data collected and the purpose of their processing shall be provided to the data subject in a concise, clear and intelligible manner.

As Controller, the Parent Company of DIMAND Group of Companies, in its regularly updated Privacy Notice, has mapped all information that needs to be disclosed at this point to all data subjects as follows:

- the identity and contact details of the Controller;
- the contact details of the Data Protection Officer, where available;
- the purposes for which the personal data is processed, and the relevant legal basis for such processing;
- the legitimate interests pursued by the Controller or by a third party (where the processing is necessary for pursuing legitimate interests);
- the recipients or the categories of recipients of personal data;
- the potential transmission of personal data to a third country or an international organization;
- the expected duration of personal data retention, or, if not possible, the criteria used to determine the said period of time;
- the rights which the data subject has on their personal data, such as the right to access, to rectification, to erasure, to restriction of processing, to object to processing and the right to data portability;
- the right to withdraw consent where the legal basis for processing is consent;

- the right to submit a complaint to a supervisory authority;
- whether the provision of personal data is a statutory or contractual obligation, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data, and concerning the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, and in such cases, where available, information about the logic involved and the significance and envisaged consequences of such processing.

B. The principle of purpose limitation

Personal data is processed only for the purpose stated at the time of collection and shall not be further processed in a manner incompatible with those purposes.

An exception to this shall be any subsequent processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

C. The principle of proportionality (data minimization)

The personal data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

D. The principle of data accuracy (data quality)

The personal data processed shall be accurate and, where necessary, kept up to date. The Group shall take all reasonable steps to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.

E. The principle of determining the duration of processing (storage limitation)

Personal data shall be stored and retained in a form that allows the identification of data subjects only for the period necessary to fulfill the purpose for which it was collected.

Storage for longer periods is permitted, insofar as the personal data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

F. The principle of data integrity and confidentiality

Personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

For this purpose, the Group has proceeded with a classification of the data it processes and the implementation of appropriate technical and organizational protection measures per classification level.

G. The principle of Controller accountability

G.I Record of Data Processing Activities

The parent Company of the Group keeps a record of the processing activities for which it is responsible (hereinafter the 'Record of Data Processing Activities'). The Record of Data Processing Activities includes at least the following information:

- the name and contact details of the Controller and, where applicable, the Joint Controller or the Controller's representative;
- the name and contact details of the Data Protection Officer;
- a description of data subject and personal data categories;
- a description of the categories of data recipients to whom the personal data has been disclosed or is to be disclosed, including recipients in third countries or international organizations;
- transfers of personal data to a third country or an international organization, including documentation of appropriate safeguards in the absence of an adequacy decision;
- the envisaged time limits for erasure of the different categories of data, where possible;
- a general description of the technical and organizational security measures, where possible;

Personal data records requiring specific protection, such as the special categories of personal data ('sensitive personal data'), where applicable, shall be stored in separate folders bearing a relevant annotation or indication in the Record of Data Processing Activities in order to ensure that the said data undergoes a data protection impact assessment.

In addition, the data receives the appropriate classification level based on content sensitivity, and the appropriate protection measures shall be implemented accordingly.

G.II Data protection impact assessment

Any person who processes personal data must carry out a data protection impact assessment whenever processing is likely to result in a *high risk* to the rights and freedoms of natural persons.

The purpose of the data protection impact assessment is to assess and mitigate the risks related to data protection. The data protection impact assessment shall be carried out before the commencement of processing.

High-risk processing activities are defined as follows:

- a systematic and extensive evaluation of personal aspects relating to the

data subject which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- the processing of sensitive personal data on a large scale;
- the systematic monitoring of publicly accessible area on a large scale, e.g. filming a public space;

The data protection impact assessment shall be adequately documented. Where the data protection impact assessment indicates that there is a high risk for data subjects, the competent supervisory authority shall be informed and consulted before the start of processing activities. The instructions received by the competent supervisory authority shall be adopted by the Company.

G. III Data protection by design and by default

In order to ensure personal data protection, the following principles are taken into account when assessing current business processes or data processing systems or when new systems are introduced.

When new data processing systems are introduced, the Controller shall ensure by design a high level of data protection. In particular, any new system and any new procedure adopted shall comply with the following principles:

- Taking technical and organizational measures to ensure the systematic and safe management of personal data during its life cycle, i.e. from collection and processing to erasure;
- Limiting the personal data collected and processed to a minimum in order to fulfill the purpose for which it was originally collected;
- Where the purpose of the processing is not hindered by the anonymization of data, data shall be anonymized to prevent identification of the data subject;
- Where personal data cannot be anonymized, safety measures shall be adopted, such as pseudonymization, encryption or access limitation;
- Access to personal data shall be granted to other persons within the Group on a need-to-know basis, so that they can fulfill specific roles, duties and responsibilities.
- Systematic quality control of personal data shall constitute an integral part of the data life cycle management;
- Data processing systems shall be adequately protected against unauthorized access through technical and organizational measures.

The Company data processing systems shall be designed in such a manner as to ensure the strictest privacy settings by default.

Extensive processing of personal data is permitted solely upon the data subject's choice or explicit consent, for instance, when the data subject opts for “Accept all Cookies” while visiting the Company’s official website.

8. Rights of the Data Subject

Under the GDPR and this Policy, data subjects have the following rights:

- Right to information;
- Right to access;
- Right to rectification;
- Right to erasure;
- Right to restriction of processing;
- Right to data portability;
- Right to object;
- Right to automated decision-making and profiling.

9. Data Transfers

Transfers to third parties

Personal data shall be transferred to third parties solely where necessary. Personal data shall be anonymized where appropriate.

A third party acting as Processor on behalf of the Company, e.g. a contractor or service provider, shall contractually commit to carrying out the processing of personal data in accordance with this Policy, through explicit reference to the relevant contract.

Cross-border transfers

Personal data shall be transferred to a third country (outside the European Union) solely if the law of that country provides for an adequate level of data protection. Where foreign law does not provide an adequate level of data protection, personal data shall only be transferred to that country if the data subject has explicitly consented to the said transfer or if data protection is ensured by an appropriate data transfer agreement.

The Group shall take all necessary technical and organizational measures to minimize the risk of accidental or intentional breach, destruction, or loss of personal data.

10. Detection and notification of personal data breaches

Any breach of this Policy, as well as of the relevant laws and regulations on personal data protection, constitutes a personal data breach. In particular, this includes the unlawful destruction, loss, alteration, unauthorized transmission/access, and processing of data without the data subject's consent or for purposes other than those stated at the time of collection.

Upon identifying a personal data breach, the person who detected it shall take all appropriate measures to protect the personal data from any additional effects and shall report the breach promptly and without undue delay to the Head of the IT Department of the Group's Parent Company.

The Head of IT Department, in cooperation with the General Directorate of Legal Services and the Compliance Unit, shall be responsible for the ongoing monitoring and systematic documentation of all personal data breaches, while assessing the underlying causes of these breaches. Moreover, additional measures shall be in place in order to remedy the breach incident and prevent any repeated violations.

The Parent Company of the Group shall notify the Data Protection Authority (DPA) of the personal data breach not later than 72 hours after the relevant executives became aware of it.

In addition, if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, the latter shall be notified without delay.

11. Controller

The Data Controller is the Parent Company of DIMAND Group of companies, namely the Company "DIMAND SOCIETE ANONYME - DEVELOPMENT AND EXPLOITATION OF REAL ESTATE AND CONSTRUCTIONS, SERVICES AND HOLDING", trading as "Dimand S.A.", seated at 115 Neratziotsis Str., Maroussi, Attica, General Electronic Commercial Registry (G.E.MI.) No 004854501000, TIN: 999631074 and official website www.dimand.gr.

12. Processors

The Parent Company of the Group engages exclusively with processors that provide sufficient assurances for the implementation of appropriate technical and organizational measures to ensure the processing of personal data, in accordance with the General Data Protection Regulation and Law 4624/2019.

Processing of personal data by a processor shall be governed by a contract, with clearly defined clauses and annexes, that is binding on the processor with regard to the said Group's Company and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects involved (e.g. partner, supplier, employee).

13. Processing of personal data by DIMAND Group of Companies

The Parent Company of DIMAND Group shall collect and process data in the context of the Group’s corporate purpose and in order to carry out the business activities of the Group’s companies.

In particular, the categories of data subjects that are subject to processing are as follows:

- Members of the Board of Directors;
- Managers;
- Employees under any kind of contract;
- Prospective employees;
- Clients;

- Business partners (e.g. suppliers, contractors, external associates, etc.)

14. Processing of special categories of personal data

Processing of 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 shall be prohibited unless:

- the data subject has given explicit consent to such processing;
- processing is necessary for the controller to carry out the obligations and exercise specific rights in the field of labor law, social security and social protection law, providing for appropriate safeguards for the fundamental rights and interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or of other natural persons, where the data subject is physically or legally incapable of giving consent;
- processing is necessary for the establishment, exercise or defense of legal claims;
- processing is necessary for reasons of substantial public interest;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment;
- processing is necessary for reasons of public interest in the area of public health (e.g. Covid-19).

The Group does not systematically process special categories of personal data and when this is the case, it is exclusively for the aforementioned listed reasons.

15. Data Protection Officer (D.P.O.)

The Group's activities do not include large-scale processing operations and the special categories of personal data processed are limited exclusively to the scope of labor law and social security law.

For the aforementioned reasons, it is not mandatory to appoint a Data Protection Officer (D.P.O.) for the Group's companies, in accordance with Article 37 of the Greek General Code of Civil Procedure.

Receiving and satisfying the requests of data subjects within a reasonable time is part of the responsibilities of the General Directorate of Legal Services.

16. Requests of data subjects

The Parent Company of the Group shall receive and manage all requests of data subjects regarding the exercise of their rights as well as any questions about personal data

through the following email address: dataprotection@dimand.gr, managed by the General Directorate for Legal Services.

The relevant executives shall receive and satisfy any requests of the data subjects as soon as possible and shall confirm the receipt of the requests through the same address.

17. Policy Breach

The potential sanctions and damages resulting from a breach of this Policy are substantial not only for the person responsible for the breach but also for the entire Group. Any breach of this Policy may lead to criminal, civil or disciplinary penalties, including but not limited to:

- Termination of contracts due to breach of terms.
- Claims for damages from partner companies or other third parties.
- Legal and administrative costs incurred in the defense of cases.
- Substantial monetary penalties.

Every General Directorate and Department is responsible for enforcing this Policy, and each employee individually is responsible for adhering to it.

Compliance with this Policy is achieved through the use of appropriate control mechanisms which include, but are not limited to, on-the-spot checks, internal and external inspections as well as feedback from the General Directorates.

18. Bringing into force and updating this Policy

This Policy shall enter into force upon the approval of the CEO, who shall become responsible for also approving any amendments to the content herein.