Data Protection Policy Document

DATA PROTECTION POLICY

COMPLIANCE WITH REGULATION (EU) 2016/679 AND
SPANISH DATA PROTECTION LEGISLATION

IDENTIFICATION OF THE DATA CONTROLLER

a) Name and contact details of the Data Controller:

- Company name/Name and surname: WORLD LEADERSHIP ALLIANCE CLUB DE MADRID
- Spanish corporate tax id. no. *CIF/NIF*: G83378000
- Activity: Strengthening inclusive democratic practice and improving the well-being of people around the world
- Contact telephone no.: (+34) 911548230
- Registered office: *Calle Mayor, 69-1ºPlanta (Palacio de Cañete), 28013*, MADRID, (Madrid), Spain
- Address for notification purposes: C*alle Mayor, 69-1ºPlanta (Palacio de Cañete), 28013,* MADRID, (Madrid), Spain
- Contact email address: rhidalgo@clubmadrid.org
- Website (URL): https://clubmadrid.org/

b) Name and contact details of the Joint Data Controller:

- There is no Joint Data Controller.

c) Name and contact details of the Data Controller's representative:

- The Data Controller's representative is established in the territory of the European Union.

d) Name and contact details of the Data Protection Officer:

- Company name/Name and surname: Audidat 3.0, SL
- Contact email address: asarmiento@audidat.com

I. PURPOSE OF THE DOCUMENT.

The Spanish Data Protection Agency expressed its desire in its Strategic Plan 2015-2019, for Data Controllers to achieve a high level of compliance with the obligations imposed on them by data protection regulations, fostering a culture of data protection that entails a clear improvement with regards to competitiveness, compatible with economic development.

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27th April 2016, relative to the protection of natural persons with regard personal data processing and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJEU L 119/1, 04-05-2016) (hereinafter GDPR), provides a modernised and accountability-based framework for data protection in Europe.

In this regard, Article 5(2) of Regulation (EU) 2016/679, establishes the principle of 'proactive accountability', according to which the controller will be responsible for (and able to demonstrate) compliance with the following principles relating to processing:

- Personal data will be processed in a lawful, fair and transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

- Personal data will be collected for specified, explicit and legitimate purposes and will not be further processed in a way incompatible with such purposes; in accordance with Article 89(1), further processing of personal data for archiving purposes in the public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes ('purpose limitation');

- Personal data will be adequate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimisation");

- Personal data will be accurate and, where necessary, kept up to date; all reasonable steps will be taken to ensure that personal data which is inaccurate in relation to the purposes for which they are processed ("accuracy") is erased or rectified without delay;

- Personal data will be kept in a form which enables identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be kept for longer periods provided that they are processed exclusively for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), without prejudice to the application of appropriate technical and organisational measures imposed by this Regulation in order to protect the rights and freedoms of the data subject ('retention time limitation');

- Personal data will be processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, by implementing appropriate technical or organisational measures ("integrity and confidentiality").

In short, the principle of "proactive accountability" requires a conscious, diligent, and proactive attitude from organisations towards all personal data processing that they carry out.

In this sense, the Management of WORLD LEADERSHIP ALLIANCE CLUB DE MADRID, with the guidance and under the supervision of its governing bodies, advocates a proactive policy of compliance, in order to ensure that the fundamental right to data protection is actively respected in the exercise of its purposes.

Accordingly, this document is drawn up in order to establish the Policy of WORLD LEADERSHIP ALLIANCE CLUB DE MADRID in relation to compliance with Regulation (EU) 2016/679 of the European Parliament and Council, on the 27th April 2016, relevant to the protection of natural persons with regard to personal data processing and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJEU L 119/1, 04-05-2016), and in the Spanish regulations on personal data protection (Organic Law, its implementing rules and specific sectoral legislation).

II. MANAGEMENT'S COMMITMENT TO DATA PROTECTION.

The Management of WORLD LEADERSHIP ALLIANCE CLUB DE MADRID (hereinafter, the Data Controller), assumes the utmost responsibility and commitment to the establishment, implementation and maintenance of this Data Protection Policy, ensuring the continuous improvement of the Data Controller with the aim of achieving excellence in relation to compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27th April 2016 on the protection of natural persons with regard to personal data processing and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJEU L 119/1, 04-05-2016), and Spanish personal data protection regulations (Organic Law, specific sectoral legislation and its implementing rules).

WORLD LEADERSHIP ALLIANCE CLUB DE MADRID's Data Protection Policy is based on the principle of proactive responsibility, according to which the Data Controller is responsible for compliance with the regulatory and jurisprudential framework that governs said Policy, and is capable of demonstrating this to the competent control authorities.

In this regard, the controller will be governed by the following principles which should serve as a guide and point of reference for all its staff with regards to personal data processing:

1. Data protection by design: the Data Controller will implement, both at the time of the determination of the means of processing and at the time of the processing itself, appropriate technical and organisational measures, such as pseudonymisation, designed to effectively implement data protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing.

2. Data protection by default: the Data Controller will implement appropriate technical and organisational measures with a view to ensuring that, by default, only personal data which are necessary for each of the specific purposes are processed.

3. Data protection in the information lifecycle: measures ensuring the protection of personal data will apply throughout the entire information lifecycle.

4. Lawfulness, fairness, and transparency: personal data will be processed lawfully, fairly and transparently in relation to the data subject.

5. Purpose limitation: personal data will be collected for specified, explicit and legitimate purposes and will not be further processed in a way incompatible with those purposes.

6. Data minimisation: personal data will be adequate, relevant, and limited to what is necessary for the purposes for which they are processed.

7. Accuracy: personal data will be accurate and, where necessary, kept up to date; all reasonable steps will be taken to ensure that personal data which are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay.

8. Limitation of the retention period: personal data will be kept in a way which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

9. Integrity and confidentiality: personal data will be processed in such a way as to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, by implementing appropriate technical or organisational measures.

10. Information and training: one of the keys to ensuring the protection of personal data is the training and information provided to staff involved in the processing of personal data. During the life cycle of the information, all staff with access to the data will be properly trained and informed about their obligations in relation to compliance with data protection regulations.

WORLD LEADERSHIP ALLIANCE CLUB DE MADRID's Data Protection Policy is communicated to all the Data Controller's staff and made available to all interested parties.

Consequently, this Data Protection Policy involves all the Data Controller's staff, who must be aware of and accept it, considering it as their own, each individual being responsible for applying it and verifying the data protection regulations applicable to their activity, as well as identifying and providing the opportunities for improvement that they consider appropriate with the aim of achieving excellence in relation to their compliance.

This Policy will be reviewed by the Management of WORLD LEADERSHIP ALLIANCE CLUB DE MADRID as many times as deemed necessary, to adapt, at all times, to the personal data protection provisions in force.

In MADRID, on FEBRUARY 16, 2024

Signed: Mr. RICARDO HIDALGO GARCÍA,
CHIEF FINANCIAL OFFICER AND LEGAL REPRESENTATIVE OF WORLD LEADERSHIP ALLIANCE CLUB DE MADRID

III. THE NEED FOR A DATA PROTECTION OFFICER.

The need for a Data Protection Delegate is detected, based on the following assumptions:

- Strengthening inclusive democratic practice and improving the well-being of people around the world

Concept of "routine and systematic observation"
The notion of routine and systematic observation of data subjects is not defined in the GDPR, but the concept of "observation of data subjects' behaviour" is mentioned in Recital 24 and clearly includes all forms of internet tracking and profiling, including for behavioural advertising purposes:

> *To determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be assessed whether natural persons are tracked on the internet, including the potential further use of personal data processing techniques consisting in profiling a natural person for the purposes, in particular, of making decisions about them or analysing or predicting their personal preferences, behaviours and attitudes.*

However, the concept of observation is not limited to the online environment and online monitoring should be seen as just one example of observation of data subject behaviour.

Article 29's Working Group understands "usual" to mean one or more of the following:
- *Continuous or occurring at specific intervals over a specific period;*
- *Recurrent or repeated at pre-determined times;*
- *Occurring constantly or periodically.*

The Working Group understands "systematic" to mean one or more of the following:
- *That it is produced according to a system;*
- *Pre-established, organised or methodical;*
- *Taking place as part of an overall data collection plan;*
- *Carried out as part of a strategy.*

Some examples of activities that can constitute a regular and systematic observation of data subjects are:
- *Operating a telecommunications network;*
- *Providing telecommunications services;*
- *Redirecting emails;*
- *Data-driven marketing activities;*
- *Profiling and scoring for risk assessment purposes (e.g. to determine credit rating, set insurance premiums, prevent fraud, detect money laundering);*
- *Keeping track of location, e.g. through mobile applications;*
- *Loyalty programmes;*
- *Behavioural advertising;*
- *Tracking of wellness, fitness and health data through wearable devices;*
- *Closed-circuit television;*
- *Connected devices, such as smart meters, smart cars, home automation, etc.*

Concept of "large scale".

Article 29's Working Party recommends that the following factors be taken into account in determining whether processing is carried out on a large scale:

- *The number of data subjects concerned, either as a specific figure or as a proportion of the relevant population;*
- *The volume of data or the variety of data elements that are processed;*
- *The duration, or permanence, of the data processing activity;*
- *The geographical scope of the processing activity.*

Examples of large-scale processing include:

- *The processing of patient data in the normal course of hospital business;*
- *The processing of travel data of people using a city's public transport system (e.g. tracking via transport cards);*
- *The processing of real-time geolocation data of customers of an international fast food chain for statistical purposes by a Data Controller specialised in the provision of such services;*
- *The processing of customer data in the normal course of business of an insurance company or a bank;*
- *The processing of personal data for behavioural advertising by a search engine;*
- *The processing of data (content, traffic, location) by telephone or internet service providers.*

Cases that do not constitute large-scale processing include:

- *The processing of patient data by a single doctor;*
- *The processing of personal data relating to criminal convictions and offences by a lawyer.*

IV. THE NEED FOR AN IMPACT ASSESSMENT.

NO need for an impact assessment is identified.

This is because **none** of the following assumptions apply:

- The Data Controller carries out a **systematic and comprehensive evaluation** of personal aspects of natural persons that is based on automated processing, such as **profiling**, and on the basis of which decisions are made that produce legal effects for natural persons or significantly affect them in a similar way.

- The Data Controller carries out **large-scale** processing of **special categories** of personal data:
  - Personal data revealing **racial or ethnic origin.**
  - Personal data revealing **political opinions.**
  - Personal data revealing **religious or philosophical convictions.**
  - Personal data revealing **trade union membership.**
  - **Genetic** data**.**
  - **Biometric** data aimed at uniquely identifying natural persons.
  - Data relating to **health** (physical or mental).
  - Data concerning the **sex life** or **sexual orientation** of natural persons.
  - Data relating to **criminal convictions and offences**, as well as to proceedings and related precautionary and security measures.

- The person in charge carries out a **large-scale systematic observation** of a **publicly accessible area.**

Concept of "systematic"
The Working Group understands "systematic" to mean one or more of the following:
- *That it is produced according to a system;*
- *Pre-established, organised or methodical;*
- *Taking place as part of an overall data collection plan;*
- *Carried out as part of a strategy.*

V. RISK ASSESSMENT.

Risk assessment

The main novelty of Regulation (EU) 2016/679 is the evolution from a model based primarily on compliance control to one based on the principle of active responsibility, which requires a prior assessment by the Data Controller of the risk that could be generated by personal data processing in order to adopt the appropriate measures based on this assessment.

As such, the Data Controller is obliged to implement appropriate and effective measures and must be able to demonstrate the compliance of the processing activities with that Regulation, the Organic Law, its implementing rules, and sector-specific legislation, including the effectiveness of such measures. Such measures must take into account the nature, scope, context, and purposes of the processing, as well as the risk to the rights and freedoms of natural persons.

Accordingly, the Data Controller will implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In assessing the adequacy of the level of security, particular account will be taken of the risks posed by the data processing, in particular as a result of accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorised disclosure of or access to such data.

In this respect, risks to the rights and freedoms of natural persons, of varying severity and likelihood, may result from the processing of data which could lead to physical, material or non-material damage, in particular in the following cases:

- In cases in which the processing is likely to give rise to problems of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social damage;

- In cases in which data subjects are deprived of their rights and freedoms or prevented from exercising control over their personal data;

- In cases in which the personal data processed reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership and the processing of genetic data, data concerning health or sex life, or criminal convictions and offences or related security measures;

- In cases in which personal aspects are evaluated, in particular the analysis or prediction of aspects relating to job performance, financial situation, health, personal preferences or interests, reliability or behaviour, status or movements, for the purpose of creating or using personal profiles;

- In cases in which personal data of vulnerable persons, in particular children, are processed;

- In cases in which the processing involves a large amount of personal data and concerns a large number of data subjects.

Risk assessment of processing operations

The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context, and purposes of the data processing. Thus, the risk should be assessed based on an objective evaluation as to whether the data processing operations pose a **low risk**, a **risk (standard risk)** or a **high risk**.

For the purposes of this data protection policy, processing operations should be considered as posing a **high risk** to the rights and freedoms of natural persons in the following cases:

1. Where the processing is likely to give rise to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic, moral, or social harm to the data subjects.

2. Where the processing is likely to deprive data subjects of their rights and freedoms or is likely to prevent them from exercising control over their personal data.

3. When non-merely incidental or accessory processing of the following categories of data occurs:

    - Personal data revealing racial or ethnic origin.
    - Personal data revealing political opinions.
    - Personal data revealing religious or philosophical convictions.
    - Personal data revealing trade union membership.
    - Genetic data.
    - Biometric data aimed at uniquely identifying a natural person.
    - Health-related data.
    - Data concerning the sex life or sexual orientation of a natural person.

- Personal data relating to criminal convictions and offences, as well as to proceedings and related precautionary and security measures.

4. Where the processing involves an evaluation of personal aspects relating to the data subjects for the purpose of creating or using personal profiles of the data subjects, in particular by analysing or predicting aspects relating to their performance at work, financial situation, health, personal preferences or interests, reliability or behaviour, financial solvency, location, or movements.

5. When data processing is carried out on groups of data subjects in a situation of special vulnerability and, in particular, minors and persons with disabilities.

6. Where there is mass processing involving a large number of data subjects or involving the collection of a large amount of personal data.

7. When personal data are to be transferred on a routine basis to third States or international organisations for which an adequate level of protection has not been declared. In this respect, the following States are considered to have an adequate level of protection:

    - **European Economic Area (EEA)** States:

        - European Union states.
        - Iceland.
        - Liechtenstein.
        - Norway.

    - **Switzerland**. Commission Decision 2000/518/EC, of 26th July 2000.

    - **Canada**. Commission Decision 2002/2/EC, of 20th December 2001, with respect to entities subject to the scope of application of the Canadian Data Protection Act.

    - **Argentina**. Commission Decision 2003/490/EC, of 30th June 2003.

    - **Guernsey**. Commission Decision 2003/821/EC, of 21st November 2003.

    - **Isle of Man**. Commission Decision 2004/411/EC, of 28th April 2004.

    - **Jersey**. Commission Decision 2008/393/EC, of 8th May 2008.

    - **Faroe Islands**. Commission Decision 2010/146/EU, of 5th March 2010.

    - **Andorra**. Commission Decision 2010/625/EU, of 19th October 2010.

- **Israel**. Commission Decision 2011/61/EU, of 31st January 2011.
- **Uruguay**. Commission Decision 2012/484/EU, of 21st August 2012.
- **New Zealand**. Commission Decision 2013/65/EU, of 19th December 2012.
- **United States**. Applicable to entities certified under the EU-US Privacy Shield. Commission Decision (EU) 2016/1250, of 12th July 2016. The list of certified entities is available on the Privacy Shield website: https://www.privacyshield.gov/list.

8. Other risk scenarios based on the Data Controller's activity.

VI. REGISTER OF INFORMATION AND TRAINING ACTIONS.

WORLD LEADERSHIP ALLIANCE CLUB DE MADRID's Data Protection Policy is based on the principle of proactive responsibility, according to which the Data Controller is responsible for compliance with the regulatory and jurisprudential framework that governs this Policy, and is able to demonstrate this to the competent control authorities.

In this regard, the Data Controller is governed, inter alia, by the principle of information and training, according to which one of the keys to guaranteeing the protection of personal data is the training and information provided to the staff involved in the personal data processing, educating employees in the so-called data protection culture.

Consequently, all staff of the entity with access to the data will be properly trained and informed about their obligations in relation to compliance with data protection regulations, receiving appropriate knowledge, training, and regular updates of WORLD LEADERSHIP ALLIANCE CLUB DE MADRID's Data Protection Policy.

In relation to the methodology of the information and training actions, a combination of different methodologies is recommended for a better assimilation of knowledge by the participants, citing the following as examples:

- Presentation of contents or master class: The teacher explains the contents in a theoretical way with the help of resources such as PowerPoint presentations.

- Simulations or case studies: The teacher proposes situations to be solved by the participants, which allow them to better assimilate the knowledge acquired.

- Group dynamics: In order to activate interaction between the participants and the teacher.

With regards to teaching staff, it is recommended that data protection and privacy professionals with previous teaching experience are used. This may fall to the Data Protection Officer of the entity responsible for the data processing, in the event that they have been designated as such. Likewise, at the end of the training action, it is advisable to carry out knowledge assessment tests for the participants.

For the purpose of internal control management of compliance with the principle of information and training within the entity, a "Register of training and informative actions" has been drawn up for staff on data protection.