Poeta Joan Maragall 1, 14th floor
28020, Madrid
taptapdigital.com

CORPORATE PRIVACY POLICY

1. Our Objective

Taptap Digital SL and its associated entities ("**Taptap**") accord paramount importance to the protection and security of personal data. Our aim is for Taptap to set a standard in privacy safeguarding. Accordingly, it is fundamental to our operations to adhere to all statutory mandates when gathering and processing personal data. These mandates specifically encompass the stipulations of the EU Data Protection Regulation and any pertinent data protection statutes.

This data protection policy delineates the tenets and protocols that Taptap enacts to preserve the rights and liberties of natural persons in relation to the processing of their personal data.

2. Our principles for the processing of personal data

In the processing of personal data, we adhere to the following principles:

- **Lawfulness**: The processing of personal data always requires a legal basis.
- **Transparency**: Every data subject should be able to understand the processing of their personal data.
- **Purpose Limitation**: The purposes for which personal data are processed must be clearly identified in advance and defined at the time of collection.
- **Data Minimisation**: The processing of personal data shall be limited to what is appropriate, factual, relevant, and necessary for the purpose of the processing. This shall also apply to the access options.
- **Accurate and Up-to-Date**: Personal data must be stored correctly and completely and kept up to date. Suitable measures should be taken to erase, correct, supplement, or update any data that are inaccurate, incomplete, or outdated.
- **Storage Limitation**: Personal data should only be stored for the time necessary for the purpose of the processing or as permitted by other legal regulations.
- **Integrity and Confidentiality**: In the processing of personal data, appropriate technical and organisational measures should be taken to adequately protect the data, particularly against unauthorised or unlawful processing, or against accidental loss and against accidental destruction or damage.

As part of the responsible execution of our commitment, we document the processing of personal data as proof of adherence to the aforementioned principles.

3. Lawfulness of data processing

Any processing of personal data is unlawful if it does not have a legal basis. Taptap processes personal data, particularly for the following legitimate reasons:

- **Execution of a contract or implementation of pre-contractual measures**, for example, processing customer data based on a contracted service or employee data based on an employment contract.
- **Compliance with a legal obligation**, for instance, data retention post-termination in accordance with tax law.
- **Legitimate interests**, such as sending advertising for services similar to those contracted (provided advertising exemption has not been requested).
- **Consent of the data subject**, for example, for profiling activities or processing health data.

Certain special categories of personal data, such as information on ethnic origin or religious beliefs, or health-related data, can only be processed with explicit consent or legal authorisation.

4. Rights of data subjects

Safeguarding the rights and liberties of natural persons in relation to the processing of their personal data is a paramount concern for Taptap. To ensure such protection, data subjects are entitled to, among others, the following rights:

- **Information**: Data subjects shall be promptly and transparently informed about the processing of their data. This applies whether the personal data is obtained directly from the subject or through third-party collection.
- **Access**: Data subjects may at any time request information about their stored/processed personal data, as well as a copy of such data.
- **Rectification**: Data subjects may request the correction or completion of their personal data if it is incorrect or incomplete, such as an erroneous name or address.

- **Erasure**: Data subjects may request the deletion of their personal data. This right is applicable unless it conflicts with existing obligations or rights, such as statutory storage obligations.

- **Restriction of Processing**: Data subjects may request that the processing of their personal data be restricted, for instance, if the data is inaccurate.
- **Objection**: Data subjects may object to the processing of their personal data for advertising purposes at any time. For other purposes, such objection is possible under certain conditions, depending on the data subject's particular personal circumstances.

- **Individual automated decision-making**: In the context of efficient business transactions, data subjects are subject to automated decision-making on a case-by-case basis only if it is lawful, for instance, in fulfilling a contract. Data subjects will be informed about the corresponding automated processing procedures.

Data subjects will receive all information related to the processing of their personal data in clear and simple language.

In the event of a personal data security breach, data subjects will be informed of the incident if legal requirements concerning risks to their rights and freedoms are met.

Data subjects are free to lodge a complaint with Taptap, contact its Data Protection Officer, the data protection supervisory authority, or a court of law to exercise their rights concerning the processing of their personal data. This policy does not restrict or affect the legal rights or legitimate claims of the data subjects.

5. Third-party processing and data transfer

Should personal data be processed by service providers or external collaborators on behalf of Taptap, appropriate data protection measures (dependent on the scope of activity) shall be enforced, for instance:

- **Third-party personal data processing**: In accordance with Article 28 GDPR, Taptap has the requisite data processing agreement in place with service providers who access personal data. Likewise, when Taptap acts as a data processor, the necessary data processing contracts are being established.

- **Transfer of functions**: If a third party is entrusted with tasks beyond personal data processing, which require their decision-making authority regarding data usage, data protection agreements (comparable to those for third-party data processing) shall be formalised with such parties. These will mandate appropriate technical and organisational measures, akin to those necessary for third-party data processing.

- **Confidentiality agreement**: If there is a risk of improper disclosure of personal data in individual cases, a confidentiality agreement will be formalised with the provider for security reasons.

Personal data may only be processed outside of the EU or viewed from outside the EU if adequate guarantees and verifications are established to ensure the security of the processing, for example, by formalising standard data protection clauses.

6. Data security, impact assessment, and technical protection measures

We implement all requisite technical and organisational measures to safeguard the processing of personal data. These particularly include mechanisms to ensure the confidentiality, integrity, and availability of personal data, as well as the resilience of systems and services.

In every data processing activity, we carefully assess any risks to the individuals' rights and privacy to choose the most suitable technical and organisational safeguards. If we identify high risks, we'll implement extra controls and measures to mitigate them effectively.

In processing personal data, the principle of 'data protection through technological design and appropriate pre-emptive data protection measures' (privacy by design/default) is observed, for instance, by pseudonymisation or data minimisation.

Technical and organisational measures are regularly reviewed for effectiveness and adjusted as necessary, in light of the latest technical advancements. This also applies to measures when involving service providers or external partners.

7. Compliance actions

This section lists the principal actions undertaken to comply with data protection regulations:

a) Personal data processing activities have been identified and inventoried with a proper **register of data processing activities**.

b) **Risk assessments** have been conducted on data processing activities to implement appropriate technical and organisational security measures commensurate with the risk level.

c) For processes likely to pose a **high risk** to the rights and liberties of data subjects, **specific impact assessments** have been carried out by Taptap.

d) In line with the principle of transparency and in accordance with Articles 13 and/or 14 of the GDPR, Taptap provides relevant information to data subjects regarding the processing conditions affecting them and their rights, through various types of **privacy notices**.

e) Following the principle of proactive accountability and to ensure compliance with regulations, Taptap has, among others, the following **protocols and standards**:

- A **Security Protocol** detailing necessary measures for continuous protection, confidentiality, integrity, availability, and resilience of processing systems and services; a rapid restoration of data availability and access in the event of a physical or technical incident; regular evaluation of the effectiveness of implemented technical and organisational measures to ensure processing security; and where appropriate, pseudonymisation and encryption of personal data.
- An **Incident Security Protocol** establishing procedures for reporting and communicating security breaches.
- A **Rights Response Protocol** outlining procedures to address the exercise of data subjects' rights.
- A **Data Erasure and Retention Protocol** setting data retention periods and data erasure responsibilities, in accordance with the principle of limiting the retention period of personal data.

8. Responsibilities and Organisation in Data Protection Matters

Taptap is accountable for the enactment of legally mandated privacy measures in the conduct of its operations.

On one hand, its governing bodies ensure the creation of necessary preconditions for the implementation of data protection requirements by its employees.

Moreover, the implementation and adherence to legal data protection requirements are supported by Taptap's Data Protection Officer.

This policy was last updated on the 25th of January, 2024.