Privacy Policy

We care about your privacy. Wojo is committed to protecting your data both when you log on to our website and when you come to work in our spaces.

Data protection and the GDPR, what does it all mean?

The European Union's General Data Protection Regulation (**GDPR**) reinforces the existing body of rules on personal data protection and helps you take control of your data by giving you a number of basic rights. Accordingly, any organisation processing personal data must assume a number of obligations.

For a better understanding of this document, '**we**' or '**our**' will be used to refer to the company WOJO and '**you**' or '**your**' will be used to refer to you individually as a natural person.

- **What is '*personal data*'?**

Any information about you as an **identified or identifiable** individual is subject to the GDPR.
For example, your contact details (*last name, first name, address)* are personal data that identify you directly. The IP address of your computer is also personal data because, when crossed with other information, it can identify you indirectly.

- **What is personal data processing?**

It is an **operation** or set of operations, carried out on personal data, regardless of the process used *(collection, recording, organisation, storage, alteration, use)*.
For example, when we collect your contact details via the online form on our website or when we use access controls for the security of our premises.

About us

At Wojo, we offer three types of '**coworking**' spaces: Wojo Spots, Wojo Corners and Wojo Sites. Depending on each site, we provide coworking spaces, dedicated offices, creative meeting rooms and common areas.

Besides workspaces, we also offer a wide range of services specially designed with you in mind. In particular, our business partners' job is to make your daily life easier, but also to promote business interactions between members of the community.

If we are to do all this, we need to collect your data and process them. When you log on to our website or visit one of our coworking spaces, we determine the reasons for and the methods in

which we process your personal data. According to the regulation, this makes us the ***data controller***.

Protecting your personal data is a priority for us and we process them in accordance with applicable regulations, namely the GDPR and the Spanish Data Protection and Digital Rights Act (Law No. 3/2018 "DPDRA").

We encourage a **culture of data protection** throughout our company in the form of strict compliance with data protection laws and by ensuring that all the personal data we control are processed securely and in a manner that is both correct and in keeping with expectations.

Our commitments

- **The principles that govern data protection**

When we process your data, we apply the key principles behind data processing:

1. **Lawfulness and fairness.** Each processing operation requires a legal basis for collecting and processing the data. When we process your data, it will usually be because we need to meet our contractual obligations to you or your employer, and in the latter case, as part of our legitimate interest with regard to you.

2. **Transparency.** We strive to provide you with information that is concise, transparent, understandable, readily accessible and written in plain language. This information is made available to you in this policy, the privacy policy on our website and the terms and conditions of the contracts we have signed with you.

3. **Purpose limitation and privacy by design.** We collect only the data required for specific, explicit and legitimate purposes, and we do not further process them in a manner that is incompatible with those purposes.

4. **Data minimisation.** All processing of personal data in our business is designed to automatically comply with the principles that govern data protection. This means that only data necessary for the purposes for which they are processed will be actually processed. We take care to restrict the amount of data processed from the outset.

5. **Accuracy.** The data collected must be accurate and, where necessary, kept up to date. Please do not hesitate to tell us if your data needs to be updated (*e.g. a change of address)* or if they are inaccurate.

6. **Limitation of storage:** we will store your personal data only insofar it is neccessary to achieve the purposes for which it has been collected.

• Ongoing compliance

In order to ensure ongoing compliance, we apply privacy protection procedures and measures throughout the processing of your data. This allows us to improve and add to the effectiveness of the measures in place across our organisation. For this purpose, we set up a regularly updated **a register of processing activities** to help identify objectives, the categories of data used and access to these data.

This ongoing compliance review is backed up by **audits**: (i) internally, through audit plans that monitor the degree of control of our operations and verify our governance, risk management and control processes; or (ii) as part of our contractual relationships, to our subcontractors or service providers to verify compliance with the principles that govern personal data protection.

We also ensure respect for privacy when we launch new activities or offer you new services. So, when we consider a processing operation 'high risk', we perform a **data protection impact assessment** (DPIA). A DPIA essentially consists of a detailed assessment of the potential risks posed by the proposed processing and of defining and implementing appropriate measures for managing those risks in accordance with data protection laws.

• A dedicated organisation

In order to strengthen the protection of your data and make it effective, we make sure we involve all our partners:

1. We have a **GDPR team** responsible for ensuring the compliance of all workspaces with applicable personal data regulations and we are on the verge of appointing a **Data Protection Officer (DPO)**.

   What is a DPO? The DPO will be responsible for ensuring that our organisation complies with the European Data Protection Regulation. The officer will be independent and have the skills and resources required for such work:
   - inform, raise the awareness of and advise our organisation and employees;
   - ensure compliance with the regulation;
   - assist with data protection impact assessments;
   - cooperate with the supervisory authority;
   - keep a data processing inventory;
   - monitor compliance on a continuous basis.

2. **Information System (IS) Managers** are responsible for the ongoing compliance of our IT equipment and infrastructure. They help the GDPR team carry out its work, providing their expertise on application security and the principles behind the structure of our IS.

3. **The legal department** offers support and legal expertise for the work carried out by the GDPR team. In particular, it plays a role in updating contractualisation and pre-contractualisation procedures and in drafting standard contractual clauses. The department is also responsible for monitoring Spanish regulatory and legislative developments that affect data protection.

4. The legal department is also assisted by **external legal counsel**, which provides support for the contractualisation and implementation of procedures in compliance with the GDPR.

5. **Our employees** are trained in and made aware of the importance of (i) taking the utmost care of your data, (ii) taking privacy into account when designing new products and services, and (iii) reporting all and any incidents involving your data. They have an obligation of confidentiality to guarantee the security and integrity of your data.

- **Supervision of data controllers' activities (subcontractors)**

We make sure that any third party we hire to process personal data on our behalf can do so in strict compliance with the GDPR and keeps your data **safe and secured**.

These subcontractors provide us with a long list of services ranging from IT and food services to assistance with the security of our premises.

However, when your data are processed by one of our **subcontractors**, we, and not the subcontractor in question, will always be the **data controllers** as far as you are concerned.

When we select a supplier, we either include certain data processing clauses in the corresponding service level agreement or we sign a separate **data processing agreement**.

- **Data transfers**

The recipients of your data are located mainly in the European Union; however, they may also be located outside the European Economic Area (EEA). For the latter, we take the security measures and legal precautions required for the security and integrity of the personal data we transfer, such as adopting the European Commission's standard contractual clauses.

- **Security and confidentiality**

As the controller of your data, we implement appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access and against any other unlawful processing. In particular, we have the following measures in place:

- **restricted access to professional files** (digital and paper formats) by authorised persons only and exclusively for their professional duties;
- **regular checks** on access authorisations;
- **obligation of confidentiality** and security for all employees and subcontractors authorised to process your data;
- **protection of workstations and tools**: automatic locking of workstations, password protection, etc.;
- **technical security measures**: traceability of accesses and incidents, regular data backup, use of anti-virus software and firewalls, penetration testing.

The measures are implemented in proportion to the risks involved in the processing and to the nature of the personal data that is to be protected.

- **Management of data protection breaches**

In the event of a security incident, we have a security **incident management procedure** in place to detect, assess and respond to data leaks or breaches.

All our employees are required to report any security issues in an incident report. If the GDPR team considers that a security incident affects personal data and involves a risk to the privacy of the data subjects, **we notify the competent authority** within 72 hours of when we become aware of the problem. We then work with said competent authority to resolve the data breach and inform you of the incident as necessary.

- **Data storage**

Your personal data will be stored for **as long as necessary** to achieve the purposes for which they were collected.

To determine the period for which your personal data will be stored, we assess the amount, nature and sensitivity of the personal data, the potential risk resulting from unauthorised use or disclosure of the personal data, the purposes for which we process your personal data and our legal obligations.

At the end of the storage period, your personal data will be **erased or archived** in accordance with legal and regulatory requirements.

Your collaboration

We can only meet our commitments if you also take care to protect your data. Help us protect the privacy and security of your personal data:

- remain vigilant when accessing Wojo spaces (*e.g. do not lend your badge to anyone, do not let unauthorised persons in);*
- adopt good IT practices when using our Wi-Fi, information systems or IT equipment; for more information, please see the Spanish Data Protection Agency's (AEPD) Guide to Privacy and Security on the Internet. Privacy protection is everyone's business. You can **report** any security risks or incidents you come across to us (*e.g. unauthorised entry into the premises, loss of your badge, phishing emails, hacking of your computer*) and should do so as soon as possible to give us the best chance to prevent or reduce the risk of a security breach.

Your rights

- **Transparent information**

As already mentioned, we are committed to transparency towards you regardless of whether the information is collected from you directly or from other sources. In both cases, our aim is to provide you with information that is easy to understand:

- concise, transparent, intelligible and readily accessible;
- written in plain language.

- **What are your rights?**

As data subject, you have the following rights:

1. **Right of access:** you can request access to the personal data we hold about you and to certain information on how they are processed. In some cases, you can request an electronic copy of your data;

2. **Right to request the rectification:** you can ask to rectify any of your data that are inaccurate or incomplete; you must then specify what the inaccuracy is;

3. **Right to restriction of processing:** under certain circumstances, processing can be restricted; you can make this request at any time and we will decide how to proceed;

4. **Right to object:** you can object to any processing based on our legitimate interest on grounds relating to your particular situation and, in any case, when we send you marketing communications;

5. **Right to erasure ('right to be forgotten'):** under certain circumstances, you can request the erasure of your personal data; when we consider, on legal grounds, that your request is admissible, we will erase your personal data without undue delay;

6. **Right to data portability:** under certain circumstances, you can ask us to provide your personal data in a commonly used,machine-readable format; if it is technically possible, you can also ask us to transmit your data to another data controller;

7. **Right to withdraw your consent:** insofar as the processing of your personal data is based on your consent, you can withdraw it at any time;

8. **Right to issue instructions** regarding the storage, erasure and disclosure of your personal data after your death. In the event of death, unless otherwise instructed by you, your relatives or others similarly associated with the deceased, and her/his heirs may contact us to request access to her/his personal data and, where appropriate, its correction or erasure.

In addition to the above- mentioned rights, we also guarantee the respect of your digital rights established in Title X of the Spanish Data Protection Act.

In order to guarantee the protection of all your rights, we have internal procedures in place to ensure a quick response to your requests free of charge.

A question? A complaint?

For more information, please see the privacy policy on our website, the data protection clause in our contract or the notice sent by your employer. If necessary, you can also consult your rights on the AEPD (Spanish Data Protection Agency) website.

You can also exercise your rights by contacting the company's data protection team at rgpd@wojo.com or by post (registered post recommended): WOJO, Service Juridique, 92, avenue Charles-de-Gaulle, 92200 Neuilly-sur-Seine.

You can also lodge a complaint about the processing of your personal data with the competent data protection authority, i.e. the *Agencia Española de Protección de Datos* (AEPD, the Spanish Data Protection Agency): Agencia Española de Protección de Datos, calle Jorge Juan, 6, 28001 Madrid.