
Group Privacy Policy



1 SCOPE AND PURPOSE OF THIS GROUP PRIVACY POLICY

The Republic Technologies group and its subsidiaries in Europe (the "Group" or "we"), take the protection of Personal data very seriously. We know privacy is important to you, and we are committed to protecting your personal information when you engage with the Group.

Personal data refers to any information related to an identified or identifiable natural person. A person is considered identifiable if they can be recognized, directly or indirectly, through elements such as their name, identification number, location data, online identifier, or specific factors related to their physical, psychological, genetic, mental, economic, cultural, or social identity (the "Personal data").

We process Personal data in accordance with applicable data protection laws, including Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons regarding the processing and free movement of personal data («GDPR»), UK Data Protection Act 2018 ("UK GDPR"), as well as any national data protection laws in the countries where we operate, ensuring a consistent level of protection across all entities within the Group

The purpose of this Group Privacy Policy (the "Privacy policy") is to explain how we collect, use, and protect your Personal data and our commitment to comply with applicable laws.

This Privacy policy applies to:

- Visitors to our websites, web applications, and communication channels;
- Customers;
- Providers;
- Content creators;
- Job applicants.

We are committed to handling your Personal data responsibly and transparently.

As the case may be, some specific data-treatments may be subject to specific privacy policies.

2 WHO COLLECTS YOUR PERSONAL DATA?

For the purpose of this Privacy policy, and according to art. 4-16 GDPR, the Group's Principal establishment, is:

- **REPUBLIC TECHNOLOGIES (INTERNATIONAL) SAS**
3750 avenue Julien Panchot - BP 80424
66004 Perpignan CEDEX- France
E-mail : legal@rpb-tech.com
Phone: +33 (0)4 68 85 12 27

The data controller is the Group's entity that determines the purposes and means of the processing of Personal data. Depending on the data-treatment concerned, the effective data controller may be:

- **REPUBLIC TECHNOLOGIES INTERNATIONAL SAS**
3750 avenue Julien Panchot - BP 80424
66004 Perpignan CEDEX- France
- **REPUBLIC TECHNOLOGIES IBERIA SLU**
Avenida Energía, 14
08630 Abrera, Barcelona - Spain
- **REPUBLIC TECHNOLOGIES FRANCE SAS**
3750 avenue Julien Panchot - BP 80424
66004 Perpignan CEDEX- France
- **REPUBLIC TECHNOLOGIES DISTRIBUTION SAS**
3750 avenue Julien Panchot - BP 80424
66004 Perpignan CEDEX- France
- **SI INTERNATIONAL SAS**
3750 Av. Julien Panchot
66004 Perpignan CEDEX, France
- **REPUBLIC TECHNOLOGIES (UK)**
LIMITED Sword House, Totteridge Road, High Wycombe, Bucks, United Kingdom, HP13 6DG
- **OCB VERTRIEBS GMBH**
Lise-Meitner-Straße 2-4
52525 Heinsberg, Germany
- **"ALTESSE" ZIGARETTENHÜLLENERZEUGUNG UND PAPIERVERARBEITUNG GESELLSCHAFT M.B.H.**
Altessesstrasse 2, A-8280 Fürstenfeld, Austria
- **REPUBLIC TECHNOLOGIES MANAGEMENT SERVICES SLU**
Gran Vía de les Corts Catalanes, 651, 3º1º
Barcelona 08010, Spain

Data are processed by the members of the Group, in compliance with this Privacy policy.

3

WHEN DO WE COLLECT YOUR PERSONAL

3.1 When you are visiting our websites, web-applications and social media pages DATA?

Forms: If the visitors use a form appearing on the websites, owned and operated by the Group (the “Websites”), the information transmitted through that form – including the contact data that are provided to process a request or respond to additional questions – are stored in the Group’s computer systems.

Customers’ accounts on E-commerce websites (as the case may be): If the Visitor of an E-commerce website is a registered Customer, he may connect to its customer accounts and/or place orders online for any of our Item(s). The information related to the account – including the contact data and the information related to the orders – are stored in the Group’s computer systems.

Cookies: Our Websites are using “cookies”. Cookies do not damage the terminal (computer, tablet, smartphone, etc.) of persons visiting the Group’s Websites, and do not contain any viruses. Cookies are used to render the Websites more convivial, efficient and secure. Cookies are small text files stored in the visitors’ terminal and stored by the browser. You can manage your choices and consents regarding the cookies through the “cookies consent management tool” of the Website. You may also configure your browser to inform you of the use of cookies, for authorization of cookies on a case by case, for acceptance of cookies in certain situations or for their general exclusion, and/or for automatic deletion of cookies when you close the browser. Deactivation of cookies may limit the website’s functionality.

Server logs: Each operator of the Websites automatically collects and stores information in the “server logs” that the users’ browsers automatically transmit, which essentially consists of technical data regarding the browser and the version thereof, the operating system that is used, the URL of reference, the name of the accessing terminal’s host, the hour of the server’s request, the IP addresses. These data are not compiled with other data sources.

Analysis tools and third-party tools: When users visit the Website, their browsing behavior may be subject to a statistical analysis, which is conducted mainly through cookies and “data analysis programs”. An analysis of users’

browsing behavior is generally anonymous. The browsing behavior cannot be traced to the particular user. Certain tools may prevent this analysis and every user may oppose it.

Specific data-treatments related to our anti-counterfeit web-application: We have developed an application that allows our final customers to check if the product they bought is genuine or counterfeit. We are led to collect pseudonymized location information to build-up statistics on the places where counterfeit products are found.

Social media pages: If a user interacts with our page on social media, the information related to its account – including the contact data and the information related to the interactions – will be made available to us by the media owner.

3.2 When the data are part of the relationship with our professional customers and providers

We are processing the Personal data that are necessary for the execution of the contracts with our customers and providers or for the enforcement of pre-contractual measures. The data transmitted by our customers/providers are processed and registered in the Group’s computer systems.

3.3 When the data are part of our recruiting campaigns

We are processing the Personal data of the job applicants that are necessary for the recruitment operations. The data transmitted by the job applicants are processed and registered in the Group’s computer systems.

WHAT ARE THE PURPOSES, LEGAL BASIS AND DATA RETENTIONS OF THESE DATA-TREATMENTS ?

On a general assessment, the Group commits itself to process the Personal data:

- for specified, explicit and legitimate purposes;
- with valid legal basis;
- and to set forth retention periods in accordance with the purpose for which personal data are collected and in accordance with the legal obligations (laws and regulations may set a minimum period during which the Group must retain Personal data).

IN PARTICULAR, WE ARE PROCESSING TO THE FOLLOWING DATA TREATMENTS ACTIVITIES:

PURPOSE	DETAILED PURPOSE (if necessary)	LEGAL BASIS	RETENTION PERIOD
Sales relationships management	Prospection operation to professional customers	Legitimate interest	3 years from the last contact with a future customer
	Non-digital prospection operation to physical persons (as the case may be)	Legitimate interest	
	Digital prospection operation to physical persons (as the case may be)	Consent	
	Customer's management	Contract execution	3 years from the end of the contract
	Accounting operations	Legal obligation	10 years
Communication and promotion operations	Necessary cookies	Legitimate interest	Most of the cookies used by the group's Websites are "session cookies" (they are automatically erased at the end of each visit), but various retention period may apply depending on the kind of cookies with a maximum of 13 months (retention periods are detailed within the cookie module).
	Non-necessary cookies	Consent	
	Moderation of our social media pages	Legitimate interest	As long as it is made available by the social media
	Recruiting content creators	Contract execution (& pre-contractual measures)	The campaign period + 3 years
Website security management	-	Legitimate interest	6 months (maximum)
Anti-counterfeit program & web-application	On a general basis	Intérêt légitime	24 months
	For some data-treatments where the Customer's participation is needed	Consent	
Providers management	Provider's management	Contract execution.	3 years from the end of the contract
	Accounting operations	Legal obligation	10 years
Quality management	-	Providers/Customers contract execution & Legitimate interest	3 years from the end of the contract
Recruiting operations	-	Legitimate interest & precontractual operations	12 months

5 WHAT KIND OF INFORMATION ARE COLLECTED?

The personal information that may be collected in the context of the processing activities listed above includes the following information:

- **Sales relationships management:** The data necessary to identify our customers and the data necessary to monitor the customers relationship (products consulted, quantity and price of products ordered, delivery address, payment information, your choices on our prospecting operations (when applicable) and any other information necessary to the sales relationship management).
- **Communication and promotion operations:** The data related to browsing information (such as device and browser used, IP address, date and time of browsing, browsing history and the data related to interactions with users on our social media pages).

Most of the Cookies used by the Group are “necessary cookies” in order to provide services in an optimized manner without technical errors.

With your prior consent, we may also use other kinds of cookies:

- Analysis cookies, which generate statistics (location of visitors, time and duration of website visits, etc.). Functional cookies, for example to facilitate interaction with social networks;
- Advertising cookies, which allow us to identify you and your preferences based on your behavior on the Internet, in order to offer you targeted advertising.

You can manage your choices and consents regarding the cookies through the “**cookies consent management tool**” of the Website

- **Recruiting content creators:** Identifying data, age group, kind of topics covered by the content creator, type of content, previous brands' collaboration experiences, motivation to collaborate, online audience;
- **Website security management:** the browser and the version thereof, the operating system that is used, the URL of reference, the name of the accessing terminal's host, the hour of the server's request, the IP addresses;

- **Anti-counterfeit program:** the fingerprint of the phone (the fingerprint is pseudonymized information that does not allow us to identify its owner), the time and location associated with the fingerprint;
- **Providers management:** the data necessary to identify our providers and the data necessary to monitor the provider relationship (products/services ordered, quantity, payment information, delivery information, satisfaction information, etc.);
- **Quality management:** the data necessary to identify our customers/providers and the data necessary to monitor the quality management (quality of products/services, respect of delays, satisfaction information, etc.);
- **Recruiting operations:** the contact information (such as name, address, phone number), the data provided on the CV (professional background, qualifications), the information related to the appreciation of the job applicant collected during the interviews and, as the case may be, the results of the tests realized during the recruitment process.

6 WHO HAS ACCESS TO YOUR PERSONAL DATA?

6.1 Employees of the Group

Personal data collected on the Group's Websites may be processed by the employees of the group companies for the purposes and under the conditions set forth hereinabove.

6.2 Third parties:

In some particular situations, Personal data thusly collected may be transmitted outside of the Group for the following purposes and under the following conditions:

- to third party agents and entrepreneurs for the purpose of providing services (for example, providers of computer services). As subcontractors having access to data, these third parties are subject to appropriate obligations with respect to data protection, and use the Personal data thusly transmitted in compliance with this Privacy policy and the applicable regulations. The Group ensures that third parties have access only to Personal data that are necessary for them to carry out their specific tasks;

- to the extent that such transmission is required by law, for example, to comply with any legal obligation (including, and without necessarily being limited thereto, to meet the requirements for tax declarations and for disclosure to legal authorities and various governmental agencies, or by virtue of a judicial injunction), or to establish, exercise or protect the existence of rights in court;
- in the event of a sale of a group company or any of its assets, which might require the disclosure of Personal data to the potential buyer up to a degree of reasonable diligence; and
- if all or part of the group is acquired by a third party, in which case the Personal data held by the Group would necessarily be disclosed to the acquiring third party.

6.3 Cross-border transfers

The Group is a worldwide enterprise operating in a number of countries. The suppliers, customers and websites are spread throughout the world. Therefore, the Websites may collect and transfer Personal data on an international scale; in other words, in some situations, the Group may transfer Personal data collected in a country outside of this country.

When Personal data are transferred to a country outside of the European Union, the Group ensures that they are protected and transferred in a way that complies with the legal and regulatory requirements. For example, data may be transferred outside of the European Union in any of the following ways:

- the country to which Personal data are transferred must be approved by the European Commission as a country that offers an adequate level of protection for Personal data;
- the addressee must have signed a contract based on “contractual type clauses” approved by the European Commission, compelling the addressee to protect the Personal data thusly transferred;
- when the addressee is located in the United States, it may be a certified member of the UE-US privacy protection system; or
- in other circumstances, the transfer of Personal data outside of Europe is allowed by law.

For a transfer of Personal data outside of the European Union, information regarding the conditions for the transfer and processing of data (including a copy of the standard clauses for the protection of data concluded with the addressees and Personal data) may be obtained by writing to the following address: **privacy@rpb-tech.com**

6.4 Third party’s plug-ins and tools

The Website may use all or part of the “web fonts” provided by Google to ensure uniform display. When the user accesses a web page, the browser downloads the required web fonts in its cache memory for correct display of texts and fonts.

To that end, the browser that is used must connect to the Google servers. Hence, Google knows that the Website was visited via the user’s IP address. The Google fonts are used for a uniform and attractive display of the Group’s website. If the browser that is used does not bear Web fonts, a font by default of the terminal is then used. More information regarding Google fonts is provided in the Google Policy.

7

DATA PRIVACY AND SECURITY

The Group’s subsidiary or entity responsible for the processing of data treats them with complete confidentiality, and is committed to protection of that confidentiality. To that end, the Group implements appropriate technical and organizational measures for avoiding the alteration and loss of data, and the unauthorized processing thereof and access thereto, in compliance with the legal obligations that apply to Processing controllers.

For reasons of security and to protect the transmission of confidential content (e.g. orders or requests sent via the Websites), the Websites may use the SSL or TLS encryption. An encrypted connection may be identified as such by the browser’s address line: it begins by “https://” instead of “http://”, and there is a padlock icon visible on the browser’ bar.

If the SSL or TLS encryption is activated, the data that is transmitted cannot be read by third parties.



DATA PROTECTION OFFICER

In accordance with the legislation, the Group appointed a Data Protection Officer for all of its entities and subsidiaries.

If you have any queries about our handling of your personal information you can contact our Data Protection Officer.

The Data Protection Officer can be reached at:

E-mail :

privacy@rpb-tech.com

Address:

**Republic Technologies Management Services
À l'attention du Délégué à la Protection des
Données (DPO)
Gran Via de les Corts Catalanes, 651, 3^{er}
Barcelone 08010, Espagne.**



THE RIGHTS RELATED TO PERSONAL DATA

In compliance with the regulatory provisions, the Group ensures that appropriate measures are taken to provide any mandatory information to persons whose Personal data are processed, in a concise, transparent, comprehensible and easily accessible way.

9.1 Nature and modes of exercising rights

In all of the following situations, when the Group collects, uses or stores Personal data, every person whose Personal data are processed has these rights, which, in most cases, may be exercised free of charge:

- The right to receive information regarding the processing of, and the access to, Personal data held by the Group; the purposes of the processing, the types of Personal data involved; the addressees or categories of addresses to which Personal data were transmitted; and the duration of retention of Personal data when such is feasible;
- The right to withdraw at any time one's consent to the processing of Personal data (when consent is the legal basis for processing). However, it is specified that, notwithstanding the withdrawal of consent, the Group has the right to process Personal data if there is a legitimate reason for doing

so. For example, it may be necessary to retain Personal data in order to comply with a legal obligation. Also, the lawfulness of the data processing up to the time of the revocation is not affected thereby;

- In some circumstances, the right to receive certain Personal data that are automatically processed – based on consent or in execution of a contract – and are transmitted to the user or a third party in a standard and machine-readable format. It is understood that the transfer of Personal data to another Processing controller, upon a user's request, may occur only when it is technically feasible to do so;
- The right to ask the Group to rectify Personal data if they are inaccurate or incomplete;
- The right to ask the Group to delete Personal data in some circumstances. However, there may be situations when a request to delete Personal data cannot be satisfied because the Group is legally required to retain them or is authorized to refuse such a request;
- The right to oppose, or request a restriction of, the processing of Personal data in some circumstances. However, there may be situations when a request for opposition or restriction of the processing of Personal data cannot be satisfied because the Group is legally required to retain them or is authorized to refuse such a request.

These rights may be exercised by sending a request by e-mail to the following address: **privacy@rpb-tech.com**.

In addition, you may at any time send to the aforementioned e-mail address any questions relating to the exercise of the aforementioned rights and, more generally, any questions relating to the processing of Personal data by the Group.

To be valid, a request must contain an electronic copy of the national identity card or passport as documentation of the applicant's identity. A request for the exercise of rights, insofar as it is validly submitted, is processed within one month of the receipt thereof.

9.2 Right to file a complaint with the Supervisory authority

Each user whose Personal data are processed by the Group has the right to file a complaint with the competent supervisory authority.

The competent supervisory authority regarding the data protection legislation is the lead supervisory authority – i.e. the authority that falls within the jurisdiction of the Group's head office in accordance with article 56.1 of the GDPR; or, if applicable, the competent supervisory authority in the country where the Group's entity operating the website and processing Personal data is located, in accordance with article 56.2 of the GDPR.

The list of competent authorities is provided below:

1. Lead supervisory authority:

France

Commission Nationale de l'Informatique et des Libertés
3 place de Fontenoy – TSA 80175
75334 Paris CEDEX 07 (France)
Tél.: +33 (0)1 53 73 2222

2. National supervisory authorities:

Allemagne

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30
D-53117 Bonn (Germany)

Autriche

Österreichische Datenschutzbehörde
Wickenburgasse 8
1080 Vienne (Austria)

Royaume-Uni

Information Commissioner's Office (ICO)
Wycliffe House
Water Lane, Wilmslow
Cheshire SK0 5 AF (United Kingdom)

Espagne

Agencia Española de Protección de Datos
C/Jorge Juan 6
28001 Madrid (Spain)

CHANGES TO THIS PRIVACY POLICY

This Privacy policy represents the Group's general commitments at the date of its publication.

The Group is committed to continuous improvement in terms of personal data protection and may therefore make changes to this Privacy policy.

We will post such changes on this page and will endeavor to notify you of any significant changes. We invite you to consult our Privacy policy on a regular basis.