Group Confidentiality Policy

Version of 4 January 2019

1 Data protection at a glance

The Republic Technologies group and its subsidiaries and affiliates in Europe (hereinafter referred to as « the Group »), the operators of websites they own (hereinafter referred to as « the websites »), take the protection of personal data very seriously. Personal data are processed in accordance with (EU) regulation 2016/679 of the European Parliament and Council of 27 April 2016 regarding protection of natural persons in the processing of personal data and in the free circulation of data (hereinafter referred to as « the General Data Protection Regulations » or « GDPR »).

The following paragraphs give an overview of how the personal data of persons who visit the Group's websites (hereinafter « the visitors or users ») are treated, and the Group's commitment to compliance with the right to privacy pursuant to the applicable regulations, particularly the GDPR. When persons use our websites, various personal data are collected. This confidentiality policy describes the data that are collected, how they are collected, and explains the ways in which they are used by the group and the purpose thereof.

For further information regarding the meaning of the terms used herein, a glossary is provided at the end of this confidentiality policy.

2 Who collects personal data

Data on the websites are processed by the operator thereof, which is a member of the Group, in compliance with this confidentiality policy. The contact data of the entity operating the website appear in the legal information section of each website.

2.1 Processing controller

The processing controller is, depending on the situation, the subsidiary or the entity of the Group that operates the website visited by the user, or with which he interacts with the entity. The controller's contact data are available on the page dedicated to legal information for each website.

2.2 Group's principal establishment

The Republic Technologies Group's principal establishment, as defined by Article 4 of the GDPR is with Republic Technologies International, at 3750 avenue Julien Panchot, 66000 Perpignan, France, and may also be contacted at the following email address: legal@rpb-tech.com

2.3 Data Protection Officer

In accordance with the legislation, the Group appointed a Data Protection Officer for all of its entities and affiliates, on the basis of his professional skills and specific knowledge of data protection law and practices, and his ability to carry out the assignments he is given.

The Data Protection Officer can be reached at the following email address:
privacy@rpb-tech.com

And at the following postal address:
Republic Technologies Management Services,
the Data Protection Officer,
Gran Via de les Corts Catalnaes,
651, 3°1° Barcelona 08010,
Spain.

3 Why do we process your personal data?

Personal data are collected when they are provided by the visitor to the website. They may consist of data provided in a website's contact form (e.g. name, email, telephone, etc.).

Other data are automatically collected by the computer systems when the websites are visited. They consist first of technical data (e.g. internet browser, operating system and hour of access to the website). These data are automatically collected as soon as the websites are visited.

Part of the data is collected to ensure the websites' error-free availability. Other data may be used to analyze the behaviour of the websites' users.

3.1 Contact form

If persons use a contact form appearing on a website, the information transmitted through the contact 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.

Personal data are processed in accordance with the regulatory provisions and on the basis of consent (Article 6.1 a) of the European Data Protection Regulation, or when the processing is necessary for the execution of a contract to which the person involved is a party or for the enforcement of pre-contractual measures taken by that person.

The data transmitted through the contact form are processed and registered in the Group's computer systems until a request for deletion thereof or a revocation of consent to the retention of data, or until retention thereof no longer serves a purpose (for example, after the processing of a request). The mandatory legal provisions, particularly the time for retention, are not affected.

3.2 Cookies

The websites use "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.

Most of the cookies used by the group's websites are "session cookies". They are automatically erased at the end of each visit. The other cookies remain recorded in the visitors' terminal until the users delete them. They facilitate recognition of the browser during subsequent visits to the Group's websites.

You may 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.

Cookies that are necessary for implementation of the electronic communication process or for the availability of certain functions wanted by certain users of the websites (e.g. purchase basket function) are stored pursuant to Article 6.1 f) of the European Data Protection Regulation – i.e. on the basis of a legitimate interest in the storage of cookies in order to provide services in an optimized manner without technical errors.

3.3 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 :

· 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 address.

These data are not compiled with other data sources.

The server logs contain data processed pursuant to Article 6.1 f) of the European Data Protection Regulation – i.e. on the basis of a legitimate interest pursued by the processing controller. The objective here is to collect and store personal data in server logs for the sole and legitimate purpose of detecting and preventing fraud and unauthorized access to the Group's computer systems, and ensuring the security thereof.

3.4 Analysis tools and third party tools

When users visit the Group's websites, their browsing behaviour may be subject to a statistical analysis, which is conducted mainly through cookies and "data analysis programs". An analysis of users' browsing behaviour is generally anonymous. The browsing behaviour cannot be traced to the particular user. Certain tools may prevent this analysis and every user may oppose it.

3.5 Data confidentiality 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.

4 Who has access to personal data

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

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 confidentiality 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.

4.1 SSL or TLS encryption

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 are transmitted cannot be read by third parties.

4.2 Cross-border transfers

The Group is a worldwide enterprise operating in a number of countries. The suppliers, customers and sites are spread throughout the world. Therefore, the sites 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

4.3 Plug-ins and tools

Google fonts

Certain websites may use all or part of the "web fonts" provided by Google to ensure uniform display. When the user accesses a webpage, 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 Group's websites were 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 confidentiality policy.

Google Maps

Certain websites may use all or part of the Google Maps service via an API. The supplier is Google Inc, 1600 Amphithéâtre Parkway, Moutain View, CA 94043, USA.

To use the Google Maps functionalities, the visitor's IP address must be stored. This information is generally transmitted to a Google server in the United States and is generally stored thereon. The operator of the Group's websites has no influence on this transmission of data.

Google Maps is used to make the websites' presentation attractive and to easily find the locations specified by the Group on the websites.

Any further information regarding the processing of user data is provided in the Google confidentiality policy.

Facebook Plug-in

Certain websites may use all or part of the plug-ins of the Facebook social network of Facebook Inc, 1601 S. California Ave, Palo Alto, CA 94304, USA. Such plug-ins are recognizable with the Facebook logo or the "I like" button, which are integrated on the Group's websites. Any further information regarding the Facebook plug-ins and the extent and purpose of the collection, storage and use of data on Facebook is provided in the Facebook declaration of data protection.

5 The duration of retention of personal data

The duration of retention of personal data varies and is determined pursuant to the following criteria:

- the purpose for which personal data are collected and retained – personal data are retained for as long as it serves that purpose; and
- the legal obligations – laws and regulations may set a minimum period during which the Group must retain personal data.

6 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.

6.1 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. 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.

Any questions related to the exercise of the aforesaid rights and, more generally, any questions related to the processing of personal data by the Group may be submitted at any time to the following address: **privacy@rpb-tech.com**
These rights may be exercised by sending a request by email to the following address: **privacy@rpb-tech.com**

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.

6.2 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. A list of competent authorities may be consulted in this document.

Glossary

The following terms used in this confidentiality policy have the following meanings:

"Independent supervisory authority": An independent public authority established by a member State by virtue of article 51 of the GDPR.

"Supervisory authority involved": A supervisory authority that is involved in the processing of personal data because:
(a) the processing controller or the subcontractor is established in the member State of that supervisory authority;
(b) the persons involved who reside in the member State of that supervisory authority are, or might be, substantially affected by the processing; or
(c) a complaint was filed with this supervisory authority.

"Lead supervisory authority": The supervisory authority of the principal or single establishment of the processing controller or the subcontractor, which has jurisdiction to act as a lead supervisory authority with respect to the cross-border processing of data effectuated by the processing controller or the subcontractor.

"Consent" by the person involved signifies consent to the processing of his personal data, which he gives freely, specifically and knowledgeably without any ambiguity through a declaration or a clear positive action.

"Addressee": A natural person or a legal entity, a public authority, an agency or any other entity to which personal data are transmitted, whether or not a third party. However, public authorities that may receive personal data in the context of a particular inquiry in accordance with the law of the Union or the Member States are not deemed to be addressees. These authorities process personal data in compliance with the rules applicable to data protection according to the purposes of the processing.

"Personal data": All information regarding an identified or identifiable natural person ("person involved"); an identifiable natural person is a person who can be directly or indirectly identified by reference to an identifier such as a name, identification number, location data or an online identifier, or based on one or more factors specific to this natural person's physical, psychological, genetic, mental, economic, cultural or social identity.

"Principal establishment": Regarding a processing controller established in several member States, the location of his central administration in the Union, unless the decisions with respect to the purposes and means of processing personal data are made in another establishment of the processing controller in the Union and this establishment is empowered to apply such decisions, in which case the establishment that made such decisions is deemed to be the principal establishment.

"Processing controller": The natural person or legal entity, the public authority, the agency or any other entity which -- alone or jointly with others -- determines the purposes and means of processing personal data. When said purposes and means are determined by law of the Union or the member States, the processing controller or the specific criteria for his appointment may be determined by law of the Union or the Member States.

"Processing restriction": The marking of stored personal data in order to limit the processing thereof in the future.

"Subcontractor": A natural person or legal entity, a public authority, an agency or any other entity that processes personal data for the account of the processing controller.

"Filing system": Any structured collection of personal data that is accessible according to specific criteria, whether it is centralized, decentralized or dispersed on a functional or geographical base.

"Third party": A natural person or legal entity, a public authority, an agency or entity other than the person involved, the processing controller, the subcontractor and persons who, under the direct authority of the processing controller or the subcontractor are authorized to process personal data.

"Processing": Any operation or set of operations, whether or not carried out by automated processes, regarding personal data or sets of personal data, such as the collection, registration, organization, structuring, retention, adaptation, modification, extraction, consultation, use, communication through transmission, distribution or any other form of availability, reconciliation, interconnection, limitation, deletion or destruction.

"Cross-border processing":
(a) the processing of personal data in establishments located in the Union in more than one Member State of a processing controller or subcontractor when the processing controller or the subcontractor is established in more than one Member State; or
(b) the processing of personal data in a single establishment of a processing controller or subcontractor, which substantially affect, or might, affect the persons involved in more than one Member State.

"User" or **"Visitor":** Any person visiting or using, with a web browser employing an http customer protocol, one or more pages of the Group's websites, whose personal data may be collected during said use or visit.

List of competent supervisory authorities:

1/ Lead supervisory authority:

Commission Nationale de l'Informatique et des Libertés
3 place de Fontenoy – TSA 80175
75334 Paris Cedex 07
Tel: +33 1 53 73 2222

2/ National supervisory authorities:

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

Austria
Österreichische Datenschutzbehörde
Wickenburgasse 8
1080 Vienna (Austria)

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

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