OUTSCALE PERSONAL DATA PROTECTION POLICY

Table of contents

Preamble

Outscale S.A.S., a simplified joint-stock company, with its principal place of business at 1 rue Royale, 319 bureaux de la Colline, 92210 Saint Cloud, France, registered at the Commercial Registry of Nanterre under number 527 594 493, performs a Processing of Personal Data as part of its activity and in accordance with this Policy.

The purpose of this Policy is to present the technical and organizational measures implemented by Outscale to guarantee a high level of protection of the processed Data, to document its compliance with the French data protection act and the General Data Protection Regulation, and to inform natural persons concerned on the manner in which Outscale processes Personal Data and the means available to them to control this processing.

ARTICLE 1. Definitions

The following terms used in this Policy, when capitalized, have contractual value and are to be interpreted as follows:

Client: any entity having subscribed, directly or indirectly through a third-party reseller, to the Services and therefore contractually linked to Outscale. The Client acts as Controller.

Contract: refers to the contractual commitment, such as the contract or the general terms and conditions accepted by the Client to benefit from the provision of the Service.

Personal Data: under Regulation (EU) 2016/679 of 27 April 2016 (see in particular Article 4), "*any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

Collected Data: any Personal Data that may prove to be relevant to the determined Purposes, such as the functions, last names, first names, postal addresses, e-mail addresses, phone numbers, logins and passwords, universities, diplomas, organization types, organization name, job title, financial data, IP address.

Sensitive Data: under Regulation (EU) 2016/679 (see Recital 51), "*Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms*". These Personal data should encompass the Personal Data related to racial or ethnic origin. Such Personal Data should not be processed unless authorized in the specific cases provided for in the Regulation.

Outscale Entities (outside the European Economic Area): the Outscale Inc. and Outscale Limited Entities are considered third parties for the purposes of this Policy.

Personal Data Collection Purposes: When Outscale is the Processor, it is the Client acting as Collector who defines the Purposes of the processing. When Outscale acts as Controller, the Personal Data are generally collected for the needs of Outscale's business.

In addition, Outscale processes Personal Data for the following purposes: to enable data subjects to request information about Outscale and its services; to enable interactive and personalized use of the website; to identify needs in order to provide better-suited services; to enable the opening and management of an account; to enable the management of Outscale marketing activities; to process candidate applications; to compile statistics on its Clients' consumption and any other Purpose related to Outscale's activity.

Data Subject: an identified or identifiable natural person to whom the Personal Data undergoing processing is related.

Policy: refers to the present document applicable to any Data Subject concerned by the Processing (including Client, user, employees, subcontractors, partners, suppliers, prospects, etc.) regarding the rules of access and use of the Services provided by Outscale.

Controller: under Regulation (EU) 2016/679, "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

Service: refers to the service provided by Outscale under the conditions referred to in the Contract.

Processor: under Regulation (EU) 2016/679, "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*".

Subprocessor: when the Processor uses the services of another Processor to carry out the Processing of the Controller's Data, the second Processor is known as a Subprocessor.

Third party: under Regulation (EU) 2016/679, "*a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data*".

Processing: under Regulation (EU) 2016/679, "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

Personal Data Transfer: transfer of data from an Outscale entity to another Outscale entity or to a Third Party located inside or outside the European Economic Area.

ARTICLE 2. Scope

This Data Protection Policy applies from May 25, 2018.

The Policy applies when Outscale is the Controller and is processing Personal Data on its behalf or when Outscale is a Processor and is processing Data on behalf of its Clients.

It is specified that Outscale acts as Processor when it processes Client Data as part of its Cloud computing Services.

This Policy applies to all Outscale infrastructure located in the European Union territory and dependent on Outscale S.A.S. (France).

ARTICLE 3. Main principles

1. **When Outscale acts as Controller:**

a. Purpose limitation

Prior to any Processing of Personal Data, Outscale must ensure that the said Processing is based on a specific, explicit and legitimate Purpose for which the Personal Data is processed.

b. Legal basis, lawfulness, fairness, transparency

When Processing Personal Data, Outscale must ensure that the Processing rests upon a legal basis.

If the Processing results from the application of a Contract, it is then considered lawful.

If the Processing does not result from the application of a Contract, Outscale must demonstrate that the Processing responds to a legitimate interest. The Purpose of the Processing must be of legitimate interest to Outscale with regard to its main activity and must not violate the privacy of the data subjects.

When the Processing does not meet the conditions set out above, Outscale must request the prior consent of the data subjects in accordance with the following cumulative conditions:

- The consent must be given with a clear and positive act (opt-in);
- The consent must be freely given;
- The consent must contain the specific, informed and unambiguous indication of the Data Subject's agreement to the Processing of Personal data.

c. Minimization of Data

The Processing of the Personal Data must be strictly necessary to the Purpose initially determined for the processing.

d. Further compatible Processing

Outscale may carry out further processing of the Data collected, provided that such processing is compatible with the Purposes for which the Data were initially collected (scientific research, statistics, etc.).

e. Data accuracy/quality

During the life cycle of the Data, Outscale must ensure that the Data is accurate and up to date.

The Client may exercise their right of rectification to update their Personal data.

f. Limitation of Data retention

Outscale must take care not to keep the Data longer than necessary for the Purposes of the processing.

g. Security measures / Integrity and confidentiality

Outscale implements security measures in order to secure its IT environment against unauthorized or illicit processing and against accidental loss, destruction or damage (depending on the context: encryption, traceability measures, access controls, backup, etc.).

Security measures to prevent access to the infrastructure on which the Data are stored

2. **When Outscale acts as Processor:**

Outscale processes Personal Data in accordance with the instructions of its Clients.

Given the specific nature of the Services provided by Outscale, the Contract and the actions of the Client in regard to the tools made available by Outscale are considered instructions.

Outscale processes the Personal Data on behalf of its Client, for the Purpose described by the Client exclusively, in accordance with the Contract that binds it to its Client, for a duration that cannot exceed the one prescribed by the Client.

The Clients have agreed in the Contract to comply with the legislation in effect.

3. **When Outscale acts as Subprocessor:**

When Outscale acts as Subprocessor, the provisions of this Policy applicable to Outscale acting as Subprocessor shall be interpreted as applying *mutatis mutandis*.

ARTICLE 4. Processing of Sensitive Data

Outscale processes Sensitive Personal Data in limited cases.

1. **When Outscale acts as Controller:**

In these limited cases, Processing is possible only under the following alternative conditions:

- The Data Subject has given their consent;
- The Data Subject is unable to give their consent, but the Processing is necessary to protect the vital interests of the Data Subject or of another person;
- The Processing is required as part of preventive medicine or as part of a medical diagnosis by a health professional under national law;
- The Data Subject has placed the Sensitive Data into the public domain themselves;
- The Processing is essential for the purpose of instituting, exercising or defending legal proceedings, provided that there is no reason to assume that the Data Subject has a compelling legitimate interest in ensuring that the Data are not processed;
- The Processing is explicitly authorized under national law.

2. When Outscale acts as Processor:

In the event Outscale is required by its Client to process Sensitive Data, the Client and Outscale shall agree upon specific security provisions suitable for the nature of the Processed Data.

ARTICLE 5. Duration of retention

1. When Outscale acts as Controller:

Outscale agrees to retain the Personal Data that it has collected in its capacity of Controller only as long as is necessary to achieve the Purpose for which they were collected.

2. When Outscale acts as Processor:

The Personal Data collected as part of the Services are retained for the entire duration of the contractual relationship between Outscale and the Client.

In the event of discontinuation of the Services and termination of a contractual relationship for any reason, the Data will be anonymized or irreversibly deleted.

3. Data sharing

It is specified that the Data shared by the Data Subject to Third Parties cannot be deleted by Outscale. It is the Data Subject's responsibility not to share confidential information, Sensitive Data, Personal Data or Data belonging to third parties.

4. Further Processing

In accordance with Personal Data protection legislation, Outscale may carry out further processing compatible with the initial Purpose of the Processing.

Outscale may use the information at its disposal to perform statistical studies, to improve its Services or to guide research and innovation in the field of Cloud computing. Thus, for this purpose, information regarding the Data Subject may be shared and published, which is acknowledged and accepted by the Data Subject. It is specified that this information will be pseudonimized to prevent a third party from identifying the Data Subject.

ARTICLE 6. Personal Data breach

1. When Outscale acts as Controller:

In the event Outscale identifies an unauthorized or unlawful access, or a use or disclosure, whether potential or actual, of the Personal Data for which it is responsible, Outscale determines if the breach must be reported to the appropriate authorities in accordance with its Data breach management procedure.

2. **When Outscale acts as Processor:**

In the event Outscale considers there has been an unauthorized or unlawful access, or a use or disclosure, whether potential or actual, of the Personal Data for which it is responsible, Outscale informs the Controller in due time.

Outscale honors any agreement between itself and the Controller regarding Data breach.

ARTICLE 7. Third Party processing

Outscale can resort to Third Parties for its own needs or as part of the services provided to its Clients.

1. **When Outscale acts as Controller:**

When Outscale resorts to Third Parties, it ensures the Third Party:

- Implements procedures to guarantee the instructions provided by Outscale are followed, by the Third Party itself and by its subcontractors;
- Informs Outscale of any request for communication of Outscale's Personal Data that the Third Party receives from another Third Party;
- Ensures their staff and subcontractors comply with the applicable legislation and sign a specific confidentiality agreement;
- Implements a procedure to inform Outscale of the requests and complaints of the data subjects it may receive as part of the Processing of Outscale's Personal Data;
- Allows Outscale to carry out Data protection audits as part of the Personal Data Processing;
- Undertakes to audit its subcontractors regularly as part of the Personal Data Processing;
- Cooperates with Outscale to assess and document the compliance of the Personal Data Processing.

2. **When Outscale acts as Processor:**

The Client is informed that:

The data centers are managed by the following companies:	- EQUINIX - INTERXION - TELEHOUSE - DASSAULT SYSTEMES
The fiber provision is managed by the following companies:	- SIPARTECH - RATP CONNECT - INTERDATA - BSO - ZAYO

The Client authorizes Outscale to require action from these Third Parties as part of the Service provision.

In the event where the Third Parties carry out a Processing of Personal Data, Outscale must obtain the same guarantees from the said Third Parties as in the event where it was Controller as in point 1 of this article.

Outscale undertakes to inform the Client in its capacity of Controller of any change regarding the addition or replacement of Third Parties carrying out Processing of Personal Data.

If the above-mentioned Third Parties cannot have access to the Client's data for technical reasons, the above provisions do not apply. This is the case for data center and fiber providers.

ARTICLE 8. Transfer of Data to third-party countries

The transfer of Personal Data from an Outscale entity acting as Controller to a Third Party located outside the European Economic Area acting as Controller or Processor is managed by a Data Processing agreement or by specific provisions set out in the Contract.

The transfer of Personal Data from an Outscale entity acting as Processor on behalf of an Outscale Client to another entity of the company located outside the European Economic Area acting as Processor is carried out by the Client, who selects the geographical area in which the Data will be processed and under their sole responsibility.

ARTICLE 9. Data subject rights

1. **When Outscale acts as Controller:**

The data subjects may require Outscale to enforce this Data Protection Policy.

If the data subjects consider that Outscale has infringed this Policy, they will have to follow the procedure described in this document.

If no amicable settlement is conceivable in regard to the disagreement, the data subjects can seek judicial remedy.

2. **When Outscale acts as Processor:**

Regarding the Processing of the Personal Data of the data subjects, the data subjects exercise their rights upon the Clients of the company.

3. **Rights of opposition, access, rectification, portability and erasure**

The data subjects have the following rights:

- Access the Data related to them and that are processed by the company;

- Ask the rectification, erasure, deletion, or limitation of inaccurate and incomplete Personal Data related to them and Personal Data for which the Purpose of the Processing is no longer legal or appropriate;

- Object to the Processing of their Personal Data at any time, except if the said Processing is required by a legislative text and provided the Data Subject proves they have a legitimate reason induced by the specific nature of the situation;

- Receive their Personal Data in a structured, commonly used and machine-readable way, in cases where the Processing is based on a Contract or on the consent of the Data Subject. If the Processing is based on the legitimate interest of the Controller or on a legal obligation, the right to portability is not mandatory;

- Not to be the subject of a decision based exclusively on automated Processing, including profiling, producing legal effects concerning them or significantly affecting them.

4. Request for information/remarks and complaints

If a user has remarks or questions regarding these rules, they can contact Outscale by e-mail: personal-data@outscale.com.

ARTICLE 10. Complaint management procedure

The data subjects shall submit their complaints according to the following complaint management procedure.

Outscale undertakes to manage these complaints within a reasonable period of time and at the latest within one month of receipt of the complaint.

This procedure will also apply at the data subjects' request to exercise their rights of access, update and deletion regarding their Personal Data.

With regard to the data subjects' complaints relating to Outscale's Clients, in case a Data Subject files a complaint directly to Outscale, the latter will inform the Client about this request, will notify the Client of all the relevant information received from the Data Subject, and will expressly notify the Client that the processing of this complaint is incumbent upon the Client.

The Data Protection Officer will receive the complaint and forward it to the relevant Outscale departments in order to resolve the said complaint.

For any information or in order to exercise your rights on the processing of your Personal Data by Outscale, you may contact the Data Protection Officer (DPO) by e-mail: personal-data@outscale.com

Or by sending a signed letter with a copy of proof of identity at the following address:

Outscale
For the attention of the Data Protection Officer
1 rue Royale, 92210 Saint-Cloud

ARTICLE 11. Privacy by default

Outscale adopts restrictions for Data protection at the start of any new project, in order to protect data subjects' privacy from the moment a new product or service is designed.

The principles and obligations of this Policy will be included in a project from its inception.

To respect privacy by design and by default, Outscale must:

- Integrate restrictions for Data protection from the design stage;
- Anticipate restrictions for Data protection and integrate these Data in the design stage of any project;
- Ensure that restrictions for privacy are taken into account at the start of all projects;
- Ensure that the commitment of a project concerning Data protection is clearly defined and identified in order to facilitate the conformity assessment and ensure full transparency regarding the data subjects;
- Ensure that restrictions for privacy are being complied with throughout the product or system life cycle, or the duration of retention of the Personal Data.

ARTICLE 12. Impact assessment

1. **When Outscale acts as Controller:**

Outscale carries on checks on the conformity of Data Processing with regard to applicable regulations.

To that end, in certain cases, Outscale may conduct a privacy impact assessment in order to:

- Identify the processings that involve a potential risk for the protection of the Personal Data;
- Assess the level of conformity of the processings that are conducted;
- Decide on corrective actions to apply in order to ensure that the Personal Data are processed in conformity with applicable regulations.

2. **When Outscale acts as Processor:**

Outscale may be asked by its Clients to cooperate and provide them with relevant information in order to conduct this privacy impact assessment.

Outscale must provide its Clients with all relevant information it possesses and remind them that they are responsible for the successful execution of the said impact assessments.

ARTICLE 13. Data Processing Record

As Controller and as Processor, Outscale commits to maintaining a record of its data processing activities.

Outscale has responsibility to ensure that any new Processing is registered in the record with the information relevant to the context of the processing.

ARTICLE 14. Cooperation with the supervisory authorities

Outscale commits to maintaining good relations with the supervisory authorities in charge of Data protection. To that end, Outscale will cooperate and allow the supervisory authorities to audit it. Outscale will also agree to follow advice on subjects that these authorities may be aware of.

Outscale will choose the supervisory authorities its best for each existing Processing.

If supervisory authorities conduct an audit on one of Outscale's sites, the Data Protection Officer will be informed forthwith.

By e-mail: personal-data@outscale.com

Or by sending a signed letter with a copy of proof of identity at the following address:

Outscale
For the attention of the Data Protection Officer
1 rue Royale, 92210 Saint-Cloud

ARTICLE 15. Training Program

Outscale commits to implementing a training program on the protection of Personal Data. The goal of this program is to ensure that Outscale employees are aware of the principles and procedures defined in this Data Protection Policy.

This training program aims at providing Outscale employees:

- Common and shared knowledge on the principles applicable during the Processing of Personal Data;
- A clear understanding of existing procedures and when and how they apply.

The training program is followed by all Outscale employees.

The training is delivered online or on-site.

ARTICLE 16. Audit

1. **When Outscale acts as Controller:**

Outscale commits to implementing organizational and technical measures for monitoring the commitments in this Data Protection Policy.

2. When Outscale acts as Processor:

Outscale provides the Controller with the necessary documentation to demonstrate compliance with all of its obligations and to enable audits, including inspections, conducted by the Controller or another auditor mandated for these audits, and to contribute to these audits.

The Controller may subsequently, at its own expense, conduct an audit on the protection measures of the Personal Data implemented by Outscale.

The Controller will have to inform Outscale, in writing, of its intention to conduct an audit and of the choice of auditors, with fifteen (15) days' notice.

This audit may be conducted by an internal organization of the Controller or by an external, independent audit firm. The latter's activities must not be competitive to Outscale's or linked to one of Outscale's competitors.

In the situation where Outscale provides unbiased justifications to question the independence and impartiality of the selected auditor, Outscale may refuse to allow this third party to conduct the audit.