GENERAL TERMS AND CONDITIONS OF SALE FOR THE SERVER-SIDE HOSTING SERVICE

Update date: May 12, 2025.

This version of the General Terms and Conditions of Sale applies to new customers from that date onward.

I. PURPOSE

These General Terms and Conditions of Sale ("**GTCS**") define the conditions under which Sirdata, a simplified joint-stock company (*Société par Actions Simplifiée*) with a share capital of €74,885.17, registered with the Paris Trade and Companies Register under number 790 193 924, having its registered office at 20 rue Saint-Fiacre, 75002 Paris, provides its customers with a server container hosting service.

Sirdata is an expert in information technology and, in its capacity as a hosting provider, offers a hosting service (hereinafter the “**Service**”) for Server Containers developed and supplied by one or more third parties not party to these GTCS (hereinafter the "**Third Parties**"), as specified in Annex 1. The intellectual property rights in the Server Containers belong to the Third Parties. Sirdata acts solely as the hosting provider for these Server Containers and is not responsible for their development or maintenance.

Use of the Service implies the unreserved acceptance of these GTCS. Acceptance of the GTCS formalizes the Client’s agreement to comply with the contractual obligations set out in this document and its Annexes. These GTCS apply to all services provided by Sirdata and shall prevail over any other conditions, unless expressly agreed otherwise in writing by Sirdata.

The Client expressly acknowledges that the Server Containers are provided by the Third Parties and that Sirdata holds no rights therein. The only contractual relationship created is between the Client and Sirdata upon acceptance of these GTCS. No contractual relationship is established between Sirdata and the Third Parties, including but not limited to the Client's use of the Server Containers.

Sirdata provides the Client with a User Account allowing access to the Server Containers and configuration of their parameters as determined by the Client. Use of this User Account is subject to the technical and security conditions outlined in the documentation provided by Sirdata.

II. MATERIAL SCOPE

These GTCS apply to any order for the Service placed by a professional client (the "**Client**"). They govern the relationship between Sirdata and its Clients and prevail over any other documents, including the Client’s general purchasing conditions, unless expressly agreed otherwise in writing.

These GTCS, together with their "Annexes", constitute the entirety of the obligations binding the Parties with respect to the provision of the Service. The GTCS are composed of the following contractual documents, listed in descending order of legal value:

- The present document;
- The Annexes to this document.

In the event of any contradiction between one or more provisions in any of these documents, the document with the higher legal ranking shall prevail.

The Annexes forming an integral part of these GTCS are as follows:

- Annex 1: Description of the Service
- Annex 2: Personal Data Processing – DPA
- Annex 3: Financial Conditions
- Annex 4: Service Level Agreement – SLA
- Annex 5: Information System Security Measures

IN LIGHT OF THE FOREGOING, THE CLIENT ACKNOWLEDGES AND AGREES TO THE FOLLOWING:

It is hereby recalled that, pursuant to Article 1112-1 of the French Civil Code, the party possessing information that is of decisive importance for the other party's consent must disclose it, provided that the other party legitimately does not know the information or places trust in its co-contracting party. Information is deemed to be of decisive importance when it has a direct and necessary connection with the content of the General Terms and Conditions of Sale (GTCS) or the quality of the parties.

Sirdata undertakes, within the limits of the information provided by the Client, to deliver recommendations tailored to the needs expressed. The Client acknowledges that it is their responsibility to provide complete, accurate, and up-to-date information concerning its technical and functional requirements in order to enable Sirdata to propose appropriate solutions.

Sirdata provides information regarding the characteristics and conditions of use of the services based on the information communicated by the Client. The Client acknowledges that Sirdata is not required to perform a comprehensive analysis of the Client's specific needs or technical environment, unless expressly agreed otherwise in the GTCS. Any recommendation issued by Sirdata is based on the information supplied by the Client, who remains solely responsible for the accuracy of such information. Sirdata undertakes to inform the Client of any limitations of the services and of any potential technical risks associated with their use. However, Sirdata shall not be held liable for any mismatch between the services provided and the Client's needs if the Client fails to provide relevant information or elects not to follow Sirdata's recommendations.

The Client agrees to actively cooperate with Sirdata by providing all information necessary for the proper performance of the services. The Client acknowledges that any insufficiency or inaccuracy in the information provided may limit Sirdata's ability to fulfil its duty to inform and advise. Under no circumstances shall Sirdata be held liable for any consequences arising from the Client's failure to provide information or insufficient cooperation.

After having carefully reviewed the Service offered by Sirdata, the Client acknowledges having received all necessary and explicit information regarding the nature, functionalities, and terms of the service. The Client declares that they accept the present GTCS with full knowledge and understanding and undertakes to comply with its terms and conditions.

Table of contents

I. PURPOSE 1

II. MATERIAL SCOPE 1

III. DESCRIPTION OF THE SERVICES 6

IV. TERM AND RENEWAL 7

V. TERMINATION 7

VI. SUPPORT AND MAINTENANCE 8

1. Technical Support 8

2. Maintenance 8

VII. PERSONAL DATA PROTECTION 9

VIII. INFORMATION SYSTEM SECURITY 10

IX. USE OF THE SERVICE 10

X. SERVICE MODIFICATION 11

XI. FINANCIAL CONDITIONS 12

1. Amount Due 12

2. Variable Costs 12

3. Payment Terms 12

4. Payment Default 12

5. Price Revision Terms 12

XII. OWNERSHIP 13

XIII. WARRANTIES 15

XIV. LIABILITY OF THE PARTIES 15

XV. INSURANCE 16

XVI. REVERSIBILITY 17

XVII. NON-SOLICITATION OF PERSONNEL 18

XVIII. CONFIDENTIALITY 18

XIX - SEVERABILITY, NO WAIVER 19

XX. FORCE MAJEURE 19

XXI. MISCELLANEOUS 20

XXII – EVIDENCE AND NOTIFICATIONS 20

XXIII – UNILATERAL AMENDMENT OF THE GENERAL TERMS AND CONDITIONS OF SALE 21

XXIV – APPLICABLE LAW AND COMPETENT JURISDICTION 21

ANNEX 1: DESCRIPTION OF SERVICES (“SERVICE”) 22

ANNEX 2 – PERSONAL DATA PROCESSING – DATA PROCESSING AGREEMENT (DPA) 26

ANNEX 3: PRICING 33

ANNEX 4: SERVICE LEVEL AGREEMENT ("SLA") 36

ANNEX 5: INFORMATION SYSTEMS SECURITY MEASURES 39

DEFINITIONS

The capitalized terms used in these GTCS, whether in singular or plural form, shall have the meaning set forth below or as defined in bold and in quotation marks within the GTCS.

Advanced Offer: refers to the Service offering related to the implementation of both GTM Server and GTM Helper.

Annex: refers to all annexes attached to these GTCS.

Applicable Data Protection Legislation: refers to all applicable laws, regulations, and directives governing the collection, processing, retention, and security of personal data, to ensure the protection of individuals' privacy. This includes the General Data Protection Regulation ("GDPR") applicable in the European Union, as well as other relevant national or international laws, such as the French Data Protection Act ("Loi Informatique et Libertés") or the California Consumer Privacy Act ("CCPA") in the United States.

Article: refers to each section of the GTCS addressing a specific subject or stating a particular provision. The Articles are sequentially numbered in Roman numerals to facilitate reference and identification within the GTCS.

Confidential Information: refers to any information of any nature, including financial, technical, or commercial, in any form and by any means, whether oral, written, magnetic, electronic, by telecommunications or computer process, owned or held by one of the Parties and disclosed to or obtained by the other Party by any means.

Data: refers to any information stored in, transmitted to, or transmitted from a Server Container via an HTTP Request.

Data Enrichment: refers to any operation involving the addition, deletion, or modification of Data, including but not limited to, incoming and outgoing HTTP headers. This process may include the integration of new information, rectification, or enrichment of existing data to make it more complete, accurate, and relevant for processing, analysis, compliance, or transfer to third-party systems.

Documentation: refers to all documentation made available by Sirdata for the use of the Service, including any publicly available documentation accessible online via the URLs defined in Annex 1.

GTCS: refers to this contractual document, its amendments, and its Annexes.

GTM Helper: refers to the feature enabling Data Enrichment.

GTM Server: refers to the hosting service on a Server.

HyperText Transfer Protocol Request or HTTP Request: refers to a message sent to a Server, containing a request method (GET, POST, PUT, DELETE, or OPTION), a URI (Uniform Resource Identifier) that identifies the target resource, request headers to specify additional parameters, and potentially request body data or query parameters in the URI, used by some methods such as POST and GET to send Data to the Server.

IP Protocol: refers to the communication protocol used for data packet routing, as defined by the Internet Engineering Task Force in RFC 791 (https://www.rfc-editor.org/rfc/rfc791.html) and RFC 2460 (https://www.rfc-editor.org/rfc/rfc2460.html).

Internet: refers to the global electronic communications network formed by the interconnection of computer networks using the IP protocol.

Personal Data: refers to any data as defined in Article 4.1) of Regulation (EU) 2016/679 of April 27, 2016 (GDPR) relating to an identified or identifiable natural person, directly or indirectly.

Server: refers to the hardware and software infrastructure provided by Sirdata to the Client to host the Server Container.

Server Container: refers to software used for hosting Tags and Data, allowing for the reception, modification, storage, and transfer of Data to third-party endpoints or terminal equipment.

Service: refers to the services described in Annex 1 "Description of Services".

Service Account: refers to the account(s) accessible via the URL(s) defined in Annex 1, allowing, in particular, the management of the Service, access to help resources, and the viewing of usage and billing statistics.

Service Levels or "Service Level Agreement" ("SLA"): refers to the Service availability commitments set out in Annex 4.

Site: in accordance with French Law No. 2004-575 of 21 June 2004 on confidence in the digital economy (LCEN), as amended and supplemented by applicable laws and regulations, including Law No. 2018-493 of 20 June 2018 on personal data protection and the GDPR, refers to any online public communication service operated by the Client, consisting of the transmission of digital data of any kind (excluding private correspondence) by any means of electronic communication, including signs, signals, text, images, sounds, or messages of any nature.

Standard Offer: refers to the Service offering related to the implementation of GTM Server.

Tag: refers to a snippet of computer code stored and executed by the Client on a Site or in a Server Container, for example, to send, store, or transfer Data to a third-party system.

User: refers to any person under the Client's responsibility (administrator, employee, representative, etc.) who has access to the Server Container, the Data, or the Service Account.

User Account: refers to a User account, accessible from the URL address https://account.sirdata.io, allowing access to the Service Account.

III. DESCRIPTION OF THE SERVICES

As a hosting service provider, Sirdata makes available to the Client one or more servers with variable capacity for the purpose of hosting and executing Server Containers. These containers enable the reception, sending, consultation, and remote storage of Data through one or more connection URLs determined by the Client, the Third Parties, Sirdata, or its subcontractors, as applicable.

In accordance with the agreement between the Parties, Sirdata undertakes to ensure the security and confidentiality of data hosted by it or by its subcontractors, implementing physical security measures for the Server(s), logical data security, and access restrictions, under a best-efforts obligation and as described in the GTCS and its Annexes.

Sirdata handles the monitoring and maintenance of the Server(s) and provides the Client with secure access to the Service Account under the conditions defined in Annex 4 "**Service Level Agreement**." The Client manages the Server Container(s), Tags, and the processing of Data via the inferface provided by the Third Parties.

The Client acknowledges that the Service involves the use of one or more software components developed by the Third Parties, and that Sirdata acts solely as a hosting provider.

IV. TERM AND RENEWAL

These GTCS take effect from the date of acceptance by the Client upon creation of the Client Account (the "**Effective Date**"). They are concluded for an initial term of twelve (12) months ("**Initial Term**") from the Effective Date, unless terminated early under the conditions provided in Article V "Termination".

Upon expiration of the Initial Term, the GTCS shall be automatically renewed for successive periods of twelve (12) months each (the "**Renewal Period**"), unless terminated by either Party in accordance with the procedures described below.

V. TERMINATION

Either Party may terminate the GTCS at the end of the Initial Term or at the end of any subsequent Renewal Period by providing the other Party with written notice of termination by registered letter with acknowledgment of receipt or by email with acknowledgment of receipt, at least three (3) months prior to the end of the current period. Termination shall take effect at the end of that period.

Sirdata may terminate the GTCS automatically, without prior notice or compensation, in the event of non-payment by the Client of any amount due under these GTCS, following a formal notice that remains unanswered for seven (7) calendar days. If the Client fails to make payment within the seven-day period, termination shall become effective automatically, without prejudice to any damages that may be claimed from the Client, including, but not limited to, contractual and legal interest on late payments.

In the event of a breach by either Party of any of its contractual obligations, the other Party may terminate the GTCS automatically after sending a formal notice that remains unanswered for seven (7) calendar days following receipt by the defaulting Party.

The notice must specify the alleged breach and the relevant contractual clause, failing which it shall be null and void. If, at the end of this period, the defaulting Party has not remedied the breach or taken appropriate measures, termination shall become effective automatically, without prejudice to any damages that may be claimed from the defaulting Party.

In the event of repeated breaches by either Party, the other Party may terminate the GTCS automatically. Repeated breaches shall be defined as three (3) occurrences, even if rectified each time. Termination shall become effective upon receipt by the defaulting Party of a letter or email (with acknowledgment of receipt) notifying termination due to repeated breaches.

In case of force majeure, as defined in Article XX "**Force Majeure**," if such event continues for more than thirty (30) consecutive calendar days, either Party may terminate the GTCS immediately, without compensation, by letter or email (with acknowledgment of receipt) sent to the other Party.

In the event of early or regular termination, regardless of the cause, contractual obligations undertaken by the Parties up to the effective date of termination shall remain due, especially with respect to the payments due by the Client. The Client also agrees to pay Sirdata any amounts corresponding to services rendered, including reversibility services, up to the date of termination and any related early termination fees.

If early termination occurs before the end of the Initial Term or a Renewal Period for reasons attributable to the Client, the Client shall pay Sirdata an indemnity equal to the amounts due through the end of the current contractual period. Such reasons may include, but are not limited to, breach of contractual obligations, failure to meet deadlines or execution conditions, or changes in the Client's legal or financial situation (e.g., liquidation, cessation of activity).

In the event of early or regular termination, Sirdata agrees, at the Client's request, to carry out reversibility services in accordance with Article XVI “**Reversibility**”.

No termination indemnity of any kind shall be due by either Party in case of regular termination under this Article, unless the termination is due to the other Party’s breach, in which case damages may be claimed by the non-defaulting Party.

VI. SUPPORT AND MAINTENANCE

1. Technical Support

Sirdata provides technical support accessible via its Service Account, in accordance with the terms set forth in Annex 4. The Client acknowledges that this support is limited to the hosting services provided by Sirdata and excludes any support or maintenance related to the Server Containers, which remain the responsibility of the Third Parties.

The Client undertakes to promptly report any malfunction and to provide complete and relevant information, including the exact circumstances under which the issue occurred. The Client is solely responsible for the accuracy of the information provided and acknowledges that any omission or inaccuracy may delay problem resolution.

The Client must also actively cooperate with Sirdata in diagnosing the issue. Any delay or failure to provide necessary information may limit the effectiveness of Sirdata’s support and release Sirdata from any liability related to the unresolved issue.

Sirdata provides 24/7 technical support. However, this availability does not guarantee immediate response outside regular business hours, as described in Annex 4. Requests will be processed based on their priority and the availability of technical staff.

Upon notification of a malfunction, Sirdata will conduct a diagnosis and take the necessary corrective actions as soon as possible and according to available resources. Sirdata does not guarantee any specific correction timeframe and provides support on a best-efforts basis, without an obligation of result.

Any fix provided by Sirdata is subject to the terms of these GTCS, particularly regarding applicable intellectual property rights.

Response times, intervention deadlines, and guaranteed service levels are specified in Annex 4.

Sirdata only provides hosting services and does not maintain the Server Containers themselves, which are developed and supplied by Third Parties. Any incident or technical problem related to the Server Containers must be resolved directly with the responsible Third Parties. Sirdata cannot be held liable for Server Container failures or their impact on the services provided.

2. Maintenance

Sirdata is responsible for corrective and evolutionary maintenance of the Server(s).

Corrective maintenance includes the correction or workaround of malfunctions occurring during normal use of the Service and related to the hosting platform.

Evolutionary maintenance includes keeping the physical and logical security systems of the Server(s) up to date, installing security updates to mitigate malicious attacks, and repairing them in the event of a failure.

Maintenance does not cover malfunctions or service interruptions resulting from: internet service providers used to access the Servers; technical issues related to the Client's infrastructure, including configuration errors or hardware/software failures not attributable to Sirdata; or third-party software used by the Client or Server Containers provided by third parties over which Sirdata has no control.

Sirdata will make all reasonable efforts to minimize the impact of corrective and evolutionary maintenance on service availability.

However, Sirdata cannot guarantee the complete absence of service interruption or temporary degradation during these periods. In the event of evolutionary maintenance (including, but not limited to, security updates) resulting in service interruption exceeding one (1) hour, Sirdata agrees to inform the Client at least seven (7) days in advance. The interruption shall not exceed two (2) hours and shall take place between 11:00 p.m. and 6:00 a.m. in the time zone where the affected Servers are located. In exceptional circumstances, Sirdata reserves the right to adjust these times, subject to immediate written notification to the Client.

Sirdata shall not be held liable for service interruptions or performance degradation related to maintenance operations, provided they are carried out in accordance with these GTCS. The Client acknowledges that certain maintenance interventions are necessary to maintain the security and performance of the services and shall not be entitled to compensation or penalties for interruptions or slowdowns resulting from such operations.

VII. PERSONAL DATA PROTECTION

The Parties warrant that they comply with the provisions of Regulation (EU) 2016/679 of 27 April 2016, known as the “General Data Protection Regulation” (GDPR), Directive 95/46/EC of 24 October 1995, French Law No. 78-17 of 6 January 1978 “Informatique et Libertés,” Directive 2002/58/EC of 12 July 2002 “ePrivacy” as amended by Directive 2009/136/EC, or any subsequent text replacing the foregoing, and more generally with all applicable data protection regulations, whenever they act as a “**Data Controller**” or “**Processor**” as defined under Applicable Data Protection Legislation.

Each Party agrees to implement logical, physical, and organizational security measures appropriate to protect the Personal Data they may process against unauthorized access, consultation, use, disclosure, or modification. In performing these GTCS, Sirdata will process Personal Data as a Processor on behalf of the Client, who acts as the Data Controller under Applicable Data Protection Legislation.

Accordingly, the following operations fall under the exclusive responsibility of the Client:

(i) The integration by the Client into its Sites of technical elements allowing the sending and receiving of Data to and from its Server Container;

(ii) The configuration, storage, execution, and maintenance of the Server Container, the Data, and the Tags;

(iii) The management and respect of individuals’ rights under the Applicable Data Protection Legislation, and the integration on the Sites of information elements and technical tools enabling the exercise of those rights and expression of choices regarding cookies, trackers, and Personal Data processing;

(iv) The definition of the purposes for processing Personal Data and their transmission to Sirdata.

In particular, the Client agrees to comply with all applicable legal and regulatory obligations arising from the implementation of Sirdata’s products and solutions under these GTCS.

Therefore, Sirdata shall not be held liable for any non-compliance with obligations that are the Client’s responsibility under this Article or under Applicable Data Protection Legislation.

Likewise, the Client shall not be held liable for any non-compliance with obligations that are the responsibility of Sirdata under this Article or under Applicable Data Protection Legislation.

The Client guarantees that it has the right to use or transmit Personal Data to Sirdata in accordance with the purpose of the GTCS. As such, the Client acknowledges that it is solely and fully responsible, thus excluding of Sirdata, for any claim, action, or damage arising from a breach of its obligations under the GTCS relating to Personal Data or failure to comply with Applicable Data Protection Legislation. Where applicable, the Client shall indemnify Sirdata against any judgment and legal costs, including reasonable attorney fees, imposed on it by a final administrative or judicial decision.

Further provisions governing the processing of Personal Data between the Parties are detailed in the data protection agreement in Annex 2.

Compliance with the obligations under this Article constitutes not only a contractual obligation but also a binding legal obligation of public order.

VIII. INFORMATION SYSTEM SECURITY

The security measures implemented by Sirdata to protect information systems, including the security of Personal Data, are detailed in Annex 5 of these GTCS. These measures include, but are not limited to, access controls, encryption, action logging, and continuous system monitoring.

Sirdata reserves the right to use subcontractors for certain components of the Service, including, but not limited to, leasing physical or virtual servers and cloud resources.

In this context, Sirdata commits to selecting only subcontractors that offer sufficient guarantees in terms of data security and confidentiality protection, in accordance with recognized information system security standards.
To this end, Sirdata requires all subcontractors to be certified under ISO/IEC 27001 or an equivalent standard for information security management. This requirement ensures that all appropriate security measures are in place to protect hosted Data against unauthorized access, alteration, disclosure, or destruction.

IX. USE OF THE SERVICE

The Client declares that it uses the Server Container(s) in compliance with the Third Parties' terms of use and their privacy or usage policies, as defined in Annex 1.

The Client agrees to comply with the terms of use and recommendations issued by Sirdata regarding the Service described in these GTCS. The Client undertakes not to store, transmit, or allow the transmission or storage of any data or information that is unlawful, contrary to laws and regulations or public order, or that infringes the rights of third parties, particularly copyrights. The Client agrees not to use the Service in a manner contrary to the applicable regulations on electronic communications.

The Client acknowledges being aware of the technical characteristics and uncertainties associated with loading times, consultation, or other transactions carried out on the Internet via the Service, due to the nature of the network, which makes it impossible to know the recipient's bandwidth, the path taken by HTTP Requests, or the availability of bandwidth.

The Client acknowledges the risks associated with the security and confidentiality of data sent and received on the Internet, including risks of intrusion and viruses. The Client assumes full responsibility for the data it sends or receives via the Service and for implementing protective and authentication measures. The Client agrees to comply with applicable regulations concerning the confidentiality of correspondence. This includes the obligation to maintain the confidentiality of communications, in written, electronic or any other form, and to refrain from any unauthorized disclosure or fraudulent interception.

The Client agrees to cooperate in good faith and without reservation with Sirdata to enable it to fulfill its obligations under the best possible conditions.

Sirdata shall not be held liable for the consequences of any misuse of the services by the Client or the inadequacy of the solutions chosen by the Client, particularly if the Client has not followed Sirdata's recommendations or failed to provide essential information for service execution.

Any technical decision made by the Client against Sirdata's advice or without prior consultation with Sirdata shall be the sole and exclusive responsibility of the Client.

Sirdata shall in no case be held liable for direct or indirect consequences, including but not limited to data loss, service interruption, or malfunctions resulting from such decisions.

The Client is solely responsible for implementing physical and logical security solutions to protect its IT system and data against unauthorized access and computer viruses. Under no circumstances shall Sirdata be held liable if any harm results from the Client’s failure to fulfill these obligations.

In the event of the use, dissemination, or storage of unlawful data by the Client, Sirdata reserves the right to suspend or terminate the Service without notice, without any compensation being due to the Client, and without prejudice to any outstanding payments. If a third party suffers damage due to such actions, Sirdata shall not be held liable.

Sirdata shall not be held responsible for the quality, performance, or potential malfunctions of Server Containers provided by Third Parties. The Client expressly acknowledges that it uses the Server Containers at its own risk and that Sirdata shall not be held liable for any loss, damage, or service interruptions resulting from the use or malfunction of software provided by Third Parties.

X. SERVICE MODIFICATION

Sirdata reserves the right, at its discretion, to modify all or part of its technical infrastructure provided that such modification aims to improve the Service. These modifications may be made without prior notice to the Client, provided they do not result in any substantial degradation of Service performance. Sirdata shall not be held liable for minor or temporary impacts resulting from such improvements.

In the event of an exceptional and significant increase in a technical specification, such as the volume of HTTP Requests sent, the Client must request in writing the allocation of additional storage or processing capacity, which will result in a new billing arrangement mutually agreed upon by the Parties.

The Client may also request the addition of supplementary services or modifications to the existing services, regardless of their nature or justification. Sirdata will then issue a supplementary or modified proposal reflecting the technical and financial impacts, the anticipated start date, the price, and any other relevant information. The Client shall accept the proposal by signing an addendum.

In all cases, Sirdata reserves the right to refuse any request to add or modify the Service, particularly if it is not technically feasible or not aligned with Sirdata’s commercial policy. Such refusal shall not entitle the Client to any compensation and shall not affect amounts already owed to Sirdata.

XI. FINANCIAL CONDITIONS

1. Amount Due

In return for the Service, the Client agrees to pay Sirdata the amount indicated in Annex 3, which corresponds to a predefined number of HTTP Requests routed to each Server Container.

This amount is invoiced monthly in arrears.

The first invoice shall include the Server installation fees and the fixed amount for the current calendar month.

2. Variable Costs

If the number of HTTP Requests routed exceeds the applicable volume tier indicated in Annex 3, Sirdata shall invoice the amounts due for the excess usage monthly in arrears.

Readings from the monitoring tool provided by Sirdata shall prevail in case of dispute.

3. Payment Terms

Invoices shall be paid by direct debit within thirty (30) days from the invoice date, except for the first invoice, which the Client agrees to pay upon signing the GTCS.

4. Payment Default

Without prejudice to any damages, a Client's failure to pay an invoice when due shall automatically result in:

(i) The application of a late payment interest rate equal to ten (10) times the legal interest rate, without prior notice, from the first day of delay in accordance with Article L441-10 of the French Commercial Code for commercial transactions;

(ii) A flat-rate recovery fee of €40 excluding VAT payable to the creditor in case of late payment, as per Article L441-10 of the French Commercial Code;

(iii) The billing of any additional bank and management fees incurred (collection follow-up, reminder letters and calls, re-presentation of rejected direct debits, etc.);

(iv) The potential suspension of the Service seven (7) days after Sirdata sends a formal notice by registered letter with acknowledgment of receipt, in accordance with the termination terms set out in Article V.

5. Price Revision Terms

Sirdata may revise the amount due, the included elements, and the method of calculating excess usage charges at any time, provided the Client is notified in writing at least thirty (30) days prior to the effective date of the revision by email. Sirdata may make multiple price revisions within a single year, provided cumulative increases do not exceed ten percent (10%) over a twelve (12)-month period.

In the event of a price revision by Sirdata, the Client may choose between two options:

(i) **Service Adjustment**: The Client may choose to adjust the services provided by Sirdata to align with the new pricing. This adjustment may include the addition of new services or enhancements to existing services based on the Client's needs. The Client has thirty (30) days from notification of the price revision to reach a written agreement with Sirdata on the new services and their financial conditions. If no agreement is reached within this period, the price revision will be applied to the initial conditions notified.

(ii) **Termination of the GTCS**: If the price increase exceeds ten percent (10%) over a year, the Client may terminate the GTCS without penalty. To do so, the Client must notify Sirdata in writing within thirty (30) days following receipt of the price revision notice. If no termination notice is received within this period, the revision shall be deemed accepted.

In the event of early termination by the Client due to a price revision, Sirdata may invoice an amount corresponding to the services provided up to the effective termination date, as well as fixed administrative fees equal to 5% of the annual fees due.

If the Client does not respond within fifteen (15) days following the notification, the price revision shall be deemed accepted.

Price revisions shall not include increases resulting from external factors such as new taxes, regulatory fees, or energy cost increases, which will be passed on directly to the Client outside the defined increase limits.

Sirdata also reserves the right to modify the nature or scope of the services provided, subject to prior notice to the Client within thirty (30) days, to adapt to technical developments, regulatory requirements, or market condition changes.

XII. OWNERSHIP

The Service, the Documentation, the Server(s), and, more generally, the entire IT infrastructure (software and hardware) implemented or developed under these GTCS, except for subcontracted components, as well as any know-how, methods, processes, or software solutions contributing to the creation, delivery, or update of the Service, are and shall remain the exclusive property of Sirdata.

No rights of any kind to the Service, the Documentation, or any know-how, method, process, or software solution are assigned or transferred to the Client under these GTCS.

The Client's Data is and shall remain its exclusive property. No rights of any kind to such Data or any know-how, method, process, or software solution belonging to the Client and contributing to the Service are assigned or transferred to Sirdata under these GTCS.

The Client grants Sirdata a non-exclusive, non-transferable, non-sublicensable, worldwide license to reproduce the Data solely for the duration of the GTCS and solely for the purpose of providing the Service.

The Client shall indemnify Sirdata against any claim or action based on the infringement of a third party's rights due to the Data provided under the Service.

If the Client is subject to legal action for infringement, unfair competition, parasitism, or violation of any third-party intellectual property rights, or any other harmful act (hereinafter the "**Action**") due to the use of the Service, the Client must inform Sirdata within thirty (30) business days of becoming aware of the Action.

Sirdata may, at its discretion, take over and control the defense of such Action. The Client agrees to cede control of the defense upon Sirdata's request.

Sirdata shall cover the amounts, costs, and damages, including reasonable attorney fees (if applicable), arising from such Action, provided that:

(i) the Customer has informed Sirdata in writing of such Action within the time period specified above, and ;
(ii) at Sirdata's request and expense, the Customer cooperates fully with Sirdata in the defense of Sirdata's interests and its own. Sirdata will retain full control and direction of the trial of the defenses and/or any decisions to terminate any Action and ;
(iii) that the Customer does not make any statement that is prejudicial or unfavorable to Sirdata and the protection of its interests.

Sirdata may, at its expense and in performance of its obligations:

(i) Obtain the Client's right to continue using the Service and Documentation, or;
(ii) Replace or modify the Service to avoid infringing third-party rights. If, in Sirdata's opinion, it is not economically reasonable or technically feasible to do so, Sirdata may notify the Client of immediate termination of the GTCS.

Sirdata must keep the Client informed of any developments and must not agree to any settlement that imposes liability or obligations on the Client without its prior written consent.

Sirdata shall not be liable, and the Client shall indemnify Sirdata, for any Actions if the Service is:

(i) Used in a manner not provided for in the GTCS or Documentation;
(ii) Used with other applications not provided or expressly approved in writing by Sirdata; or
(iii) Modified by the Client or a third party without Sirdata's written consent.

Sirdata shall not be liable for infringement if such infringement arises from the Client's failure to comply with the GTCS or applicable regulations.

If the Client or a third party continues using any part of the Service despite Sirdata's request to cease such use or to replace or modify the Service, Sirdata shall not be held liable. In such a case, the Client shall bear all amounts, costs, and damages, including legal fees, related to any resulting Action against Sirdata and/or the Client.

Without limiting the foregoing, the Client agrees not to and shall not permit any third party to:

(i) Lend, lease, sell, assign, or otherwise transfer rights in the Service or Documentation;
(ii) Use, publish, transmit, or introduce any device, software, or routine that interferes with or attempts to interfere with the Service;
(iii) Use the trademarks, trade names, service marks, logos, domain names and any other distinctive sign or any other copyright or proprietary right associated with the Service, for any purpose, without the express written permission of Sirdata, nor;
(iv) Register, attempt to register or assist anyone else in registering any trademark, trade name, logo, domain name or other distinctive sign, copyright or other proprietary right associated with Sirdata other than in the name of Sirdata, or;
(v) Remove, obscure or alter any copyright, trademark or other proprietary rights notices appearing in the Service, or on any other items included therein, nor;
(vi) Seek, in any proceeding initiated during the term of this TOS or for one year after such term, any injunction relating to any part of the Service based on patent infringement.

XIII. WARRANTIES

The Parties declare and warrant that they have the legal capacity and authority to enter into these GTCS. They further declare that they comply and shall continue to comply with all applicable legal and regulatory provisions related to their activities during the term of these GTCS.

Sirdata guarantees the availability of the Server(s) under the conditions specified in Appendix 4. This guarantee exclusively covers technical malfunctions that are directly attributable to Sirdata's contractual obligations under the present GTC. On the other hand, incidents or service interruptions resulting from external factors or factors beyond Sirdata's responsibility, such as problems related to third parties, unauthorized interventions, or cases of force majeure, do not fall within the scope of the guarantee specified in Appendix 4.

XIV. LIABILITY OF THE PARTIES

Each Party shall be liable for the direct consequences of its own faults, errors, omissions, or breaches of the provisions of these GTCS and its Annexes that result in direct damage to the other Party. However, the liability of each Party shall be strictly limited to proven direct damages.

Sirdata shall not be held liable for indirect, consequential, or intangible damages suffered by the Client, such as loss of profit, loss of revenue, loss of data, or business interruption, resulting from the performance or non-performance of these GTCS.

The Client acknowledges that certain components of the Service, notably the Server Container management software, are provided by third parties such as, but not limited to, Google, over whom Sirdata has no direct control. Consequently, Sirdata shall not be held liable for malfunctions, interruptions, or performance deficiencies related to these third-party services. Any claim in this regard must be addressed directly to the relevant third parties. Sirdata will make its best efforts to facilitate to facilitate cooperation but shall not be held liable for third parties actions.

As a result, Sirdata cannot guarantee continuous access to the Client's Data, although it undertakes to make all reasonable efforts to ensure Service availability and performance, within the limits of its obligations as defined in these GTCS.

Sirdata shall not be liable for interruptions or slowdowns caused by the Internet service provider or by a case of force majeure as defined in Article XX. In the event of force majeure, Sirdata shall be exempt from liability for any interruptions or degradation of service quality that may impact the Client's activity.

The Client is informed that service interruptions are necessary for server maintenance. In this regard, Sirdata undertakes to comply with the procedures described in Article VI (“SUPPORT AND MAINTENANCE”) and to provide the Client with reasonable notice to allow for anticipation of any disruptions. Sirdata shall not be liable for any direct or indirect damage or financial loss (such as loss of income or opportunities) resulting from such interruptions.

Sirdata implements appropriate security measures to ensure the confidentiality and integrity of Data, in accordance with the provisions of these GTCS. However, Sirdata shall not be held liable for any alteration, destruction, or unauthorized access to Data caused by the Client or by a third party who gained access using the Client’s credentials.

In the event of a breach of integrity or confidentiality of Data directly attributable to proven fault by Sirdata, Sirdata’s liability shall be limited to direct damages suffered by the Client, up to the amount actually received by Sirdata under the current contractual period. Under no circumstances shall Sirdata be liable for indirect damages such as loss of profits, business opportunities, or data.

The Client agrees not to use the Service on behalf of a third party and shall act solely in its own name and interest. The Client has no authority to bind Sirdata in any way, directly or indirectly. Nothing in these GTCS shall be construed as creating a relationship of agency, partnership, affiliation, representation, or subordination, nor any employer-employee relationship. Consequently, Sirdata shall not be liable for any actions, decisions, or commitments made by the Client to third parties or other party, within the use of the Service.

Each Party shall be liable for direct damages caused by its failure to fulfill its obligations under these GTCS. The total liability of each Party for damages resulting from the performance or non-performance of its contractual obligations shall be limited to the total fees actually paid by the Client during the twelve (12) months immediately preceding the event giving rise to the claim. This limitation applies to all claims, whether contractual, tortious (including negligence), or based on any other legal ground.

The Parties expressly agree that liability for indirect, consequential, or intangible damages, such as loss of profit, revenue, data, or business interruption, is excluded from this clause, except in cases of gross negligence or willful misconduct by the liable Party.

However, this limitation shall not apply:

(i) To breaches of confidentiality or security of Personal Data, for which each Party agrees to take all necessary measures to protect the rights of data subjects, in compliance with applicable regulations;
(ii) To damages caused by a serious breach of the security or confidentiality obligations specified in these GTCS;
(iii) To third-party claims related to the Client's use of the Service, for which the Client shall indemnify Sirdata for any resulting damages, costs, or judgments, provided that Sirdata informs the Client in a timely manner and fully cooperates in the defense of its interests.

The Client and Sirdata agree to indemnify and hold each other harmless from any third-party claims, proceedings, or actions based on civil torts, including unfair competition, parasitism, defamation, breach of confidentiality obligations, or any other harmful act (a "**Third-Party Claim**") arising in connection with use of the Service.

If a Third-Party Claim is brought against either Party, that Party agrees to:

(i) Immediately notify the other Party in writing within a reasonable timeframe;
(ii) Allow the other Party to actively participate in the defense, and if applicable, take control of the defense at its own expense;
(iii) Not admit liability or propose settlement without the prior written consent of the other Party.

The Parties agree to fully cooperate in the defense or settlement negotiations. Neither Party shall be liable if the Third-Party Claim arises from use of the Service in a manner not compliant with the GTCS or from combination with applications not provided or approved by the defending Party.

XV. INSURANCE

Sirdata and the Client declare that they have taken out and will maintain in force, with reputable and solvent insurance companies, all necessary insurance to cover the risks related to the performance of their respective obligations under these GTCS. These insurances cover, without limitation: (i) professional liability, (ii) material and immaterial damages, and (iii) damages caused to third parties.

At the written request of either Party, the other Party undertakes to provide a valid insurance certificate specifying the scope of coverage and the insured amounts.

This certificate must be provided within a maximum of 15 days from receipt of the request.

Each Party undertakes to maintain the subscribed insurance throughout the duration of these GTCS. In the event of substantial modification, termination, non-renewal, or significant reduction of coverage, the affected Party must inform the other Party within 10 business days from notification by its insurer. The impacted Party may, if it wishes, request corrective measures to restore equivalent coverage.

The Parties agree to review the adequacy of the insurance coverage annually to ensure that new or increased risks are properly covered, particularly in case of changes in the scope of Services or applicable laws and regulations.

In the event of failure to subscribe to or maintain the required insurance under these GTCS, the defaulting Party shall be solely responsible for the financial consequences of any loss. The other Party may, at its discretion, terminate the GTCS without notice or compensation.

XVI. REVERSIBILITY

Upon written and explicit request by the Client, and where technically feasible and subject to additional fees, Sirdata agrees to perform a transfer service of the Server Container(s) used by the Client to the system designated by the Client. This service is conditional upon the Client ensuring in advance the technical compatibility of the selected systems with the Server Containers. Sirdata shall not be held liable for any incompatibility or malfunction resulting from the Client's technical choices.

In case of termination or expiration of these GTCS, for any reason, Sirdata agrees, upon written request by the Client, to return or destroy all Personal Data and Client data stored on the servers, under the following conditions:

(i) **Data return**: Sirdata shall return all data to the Client in a standard format confirmed in writing (email) with the Client within 30 days following the termination date of the GTCS. The Client is responsible for ensuring that its systems are compatible with the format of the returned data. Sirdata shall not be liable for any incompatibility resulting from technical choices made by the Client.

(ii) **Data destruction**: Upon express request by the Client, Sirdata agrees to destroy the data within sixty (60) days after the termination of the GTCS. A certificate of destruction shall be provided to the Client within five (5) business days following the destruction of the data.

The Client is responsible for ensuring its systems are compatible with the returned data. Sirdata is only bound by an obligation to return data and shall not be liable for any incompatibilities preventing reception.

Sirdata may also, upon written request by the Client, provide additional technical assistance to facilitate the implementation of reversibility, either for the Client or for a third party designated by it. These additional assistance services will be billed separately in accordance with the pricing specified in Annex 3 – Professional Services and require prior agreement between the Parties on the terms and timelines of the intervention.

The above-mentioned reversibility services shall only be provided if:

(i) The Client has made the request no later than thirty (30) days following the termination or expiration of the GTCS;
(ii) All amounts due by the Client to Sirdata have been paid;

(iii) The Client actively cooperates with Sirdata and provides all necessary technical information and logistical support to facilitate the operations.

Sirdata undertakes to make all reasonable efforts to ensure proper execution of reversibility services within the agreed timeframes. However, Sirdata shall not be held liable for:

(i) Any malfunction or incompatibility resulting from the system selected by the Client or designated third party;
(ii) Any delay or failure to implement reversibility due to external or technical factors beyond Sirdata's control;
(iii) Any indirect loss, data loss, or loss of earnings related to service interruption during the reversibility period.

If the Client fails to meet its cooperation obligations or has not settled all due amounts by the termination date, Sirdata reserves the right to suspend any reversibility service until these conditions are met. After three (3) instances of non-compliance, Sirdata shall be permanently released from any reversibility obligation without compensation to the Client.

XVII. NON-SOLICITATION OF PERSONNEL

Each Party agrees not to solicit, directly or indirectly, or hire any employee of the other Party who was involved, directly or indirectly, in the performance of these GTCS, without the prior express written consent of the other Party. This obligation shall apply during the term of the GTCS and for twelve (12) months following its termination or expiration, regardless of the cause.

This non-solicitation obligation also applies to the subcontractors, service providers, and partners of either Party involved in the performance of the GTCS. No Party may recruit or solicit employees or contractors of the other Party's subcontractors or partners without prior written consent.

In the event of a breach of this obligation, the breaching Party agrees to pay the other Party a lump sum indemnity equal to twelve (12) months of the gross monthly salary of the concerned employee or contractor, calculated based on the last monthly gross remuneration prior to departure. This indemnity is due independently of any other compensation the injured Party may claim for the damages incurred.

The Parties agree that this restriction shall not apply in the case of unsolicited applications or hires through public job postings where the employee or contractor responds independently, without any active solicitation by the hiring Party.

XVIII. CONFIDENTIALITY

Each of the Parties undertakes to (i) keep confidential all information it receives from the other Party, and in particular to (ii) not disclose the Confidential Information of the other Party to any third party, other than employees or agents with a legitimate need to know such information; and (iii) to use the Confidential Information of the other Party solely for the purpose of exercising its rights and performing its obligations under these GTCS. Notwithstanding the obligations mentioned above, neither Party shall have any obligations with respect to Confidential Information which:

(i) is or becomes publicly available other than through a breach of these GTCS; or
(ii) has been independently developed by the receiving Party without access to the Confidential Information; or
(iii) was already known to the receiving Party prior to disclosure, without any breach of a confidentiality obligation; or

(iv) has been lawfully obtained from a third party not subject to a confidentiality obligation; or

(v) must be disclosed pursuant to a law, regulation or court order. In such case, the Party compelled to disclose shall notify the other Party in writing prior to any disclosure, unless such law or decision prohibits such notification.

Upon expiry or termination of these GTCS, and upon the express request of one of the Parties, the other Party undertakes to return or destroy all copies of documents and media containing Confidential Information of the other Party, within a reasonable period of time. Such return or destruction shall be confirmed in writing to the requesting Party.

Each Party undertakes to ensure that its personnel, subcontractors and any other person or entity involved in the performance of these GTCS comply with the provisions of this confidentiality clause. Each Party remains liable for any breach of these obligations by the third parties it has involved.
The Client expressly authorises Sirdata to mention its name and/or brand as a business reference, and to reproduce these elements in its promotional materials (websites, brochures, presentations), to the exclusion of any other use.

The confidentiality obligations set forth in these GTCS shall remain in force for a period of two (2) years following the termination or expiry of the GTCS, regardless of the cause. During this period, the Parties undertake not to disclose any Confidential Information, except with the prior express authorisation of the other Party or pursuant to a legal obligation.

XIX - SEVERABILITY, NO WAIVER

In the event that any provision of the GTCS is declared illegal, void or unenforceable by virtue of law, regulation or court decision, such declaration shall in no way affect the validity and enforceability of the other provisions of the GTC, which shall be interpreted so as to give effect to the intention of the Client and Sirdata as originally expressed and enforced to the fullest extent legally possible. The remaining provisions shall be construed so as to reflect, as far as possible, the original intent of the Parties, and enforced to the maximum extent permitted by law.

The fact that Sirdata does not invoke any of its rights or the Client's breach of any provision of these GTC shall not be interpreted as a waiver by Sirdata of its right to invoke such right or breach in the future, or of any other right or breach under the GTC. Any waiver or tolerance shall only be effective if made in writing and signed by Sirdata.

The original language of the GTC is French. In the event that translated versions of the GTC are made available in other languages and in case of contradiction or differing interpretation between the translated version and the French version of the GTCS, the French version shall prevail.

XX. FORCE MAJEURE

Neither Party shall be liable for any failure or delay in the performance of its obligations under these GTCS due to the occurrence of a force majeure event, as defined in Article 1218 of the French Civil Code and established by case law of the French courts. The following shall be considered as events of force majeure, without this list being exhaustive: intervention by civil or military authorities, fires, natural disasters, a state of war, riots, acts of terrorism, a pandemic, a total or partial interruption of telecommunications or electricity networks, as well as labour disputes such as strikes or lock-outs.

In case of a force majeure event, the affected Party must inform the other Party, immediately and in writing, of the occurrence of the force majeure event and describe the nature, the foreseeable impact on the execution of the contractual obligations and the estimated duration of such impact.

The performance of the obligations affected by the force majeure event shall be suspended for the entire duration of said force majeure event. The Party prevented from performing due to the force majeure shall make every effort to mitigate the effects of the event and shall take reasonable measures to resume performance of the GTCS as soon as possible and under the best possible conditions once the force majeure event has ended.

If the force majeure event continues for more than fifteen (15) calendar days following notification, the Parties shall consult to assess the consequences of the situation and consider, if possible, an alternative solution allowing the continuation of the performance of the GTC.

If the force majeure event persists for a period exceeding thirty (30) consecutive days, either Party shall have the right to immediately terminate the GTC, without notice, by sending a registered letter with acknowledgment of receipt to the other Party. Such termination shall take effect without the need for any judicial formality and shall not give rise to any compensation or damages for either Party.

XXI. MISCELLANEOUS

Entire Agreement: These GTCS and its Annexes constitute the entire agreement between the Parties and supersede any prior agreements or understandings, whether oral or written, relating to the same subject matter.

Severability: If any provision of these GTCS is held to be invalid or unenforceable, such provision shall be interpreted in a manner consistent with applicable law to reflect, as closely as possible, the Parties' original intentions. The remaining provisions shall remain in full force and effect.

No Waiver: The failure of either Party to exercise any right or remedy provided under these GTCS shall not constitute a waiver of such right or remedy. Any waiver must be in writing and signed by the waiving Party.
Assignment: Neither Party may assign or transfer, in whole or in part, the rights or obligations arising from these GTCS without the prior written consent of the other Party, except to an affiliate or in the context of a merger, acquisition, or transfer of all or part of its assets.

Publicity: Unless otherwise agreed in writing, Sirdata may mention the Client's name and use its logo in its commercial references, presentations, and client listings. The Client may object at any time by notifying Sirdata in writing.

Relationship of the Parties: Nothing in these GTCS shall be construed as creating a joint venture, partnership, or employer-employee relationship between the Parties. Each Party acts in its own name and on its own behalf.

XXII – EVIDENCE AND NOTIFICATIONS

All data, information, files and any other digital element exchanged between the Parties shall constitute admissible, valid and enforceable evidence, having the probative value of a private deed, in accordance with the provisions of Articles 1365 and 1366 of the French Civil Code. These digital elements shall be admissible in court and within the context of any dispute between the Parties. The Client undertakes not to contest the admissibility, validity, enforceability or probative value of the aforementioned elements, solely on the grounds of their electronic nature. The Parties agree that these elements shall be legally valid and enforceable in the same manner as a physical written document and may be produced as evidence in the event of a dispute.

The Parties undertake to implement the technical and organizational means necessary to ensure the security, authenticity and integrity of the digital elements exchanged, in order to guarantee their admissibility as evidence. Any falsification or alteration of the digital elements may be invoked as grounds for nullity.

Any notification or official communication required within the framework of the GTC must be made in writing, either by registered letter with acknowledgment of receipt, or by email to the following address: csm@sirdata.com.

The Parties agree that notifications made by electronic means shall have the same enforceable value as those made by postal mail, provided that the electronic acknowledgment of receipt is kept by the sender as evidence.

XXIII – UNILATERAL AMENDMENT OF THE GENERAL TERMS AND CONDITIONS OF SALE

Sirdata undertakes to use its best efforts to regularly improve the Service.

Consequently, Sirdata reserves the right to amend and update at any time and without notice these General Terms and Conditions of Sale. Any modification shall be immediately effective upon the posting of the revised versions of the General Terms and Conditions of Sale on the “Sirdata Account” and “Server-Side GTM Portal” websites. You are therefore advised to regularly check the latest version of the General Terms and Conditions of Sale.

Your use of the Service 30 days after the update of these General Terms and Conditions of Sale shall constitute acceptance thereof.

XXIV – APPLICABLE LAW AND COMPETENT JURISDICTION

The GTCS are expressly subject to French law, without regard to conflict of law rules which could lead to the application of another legislation.

Any dispute relating in particular to the formation, validity, interpretation, signature, existence, performance or termination of the Agreement shall be subject to French law. In the event of a dispute or claim arising from or in connection with this Agreement, the Parties undertake to negotiate in good faith with a view to reaching an amicable settlement.

In the event of failure or absence of settlement after a period of 90 days, the Parties may refer the matter solely and exclusively to the Commercial Court of Paris.

ANNEX 1: DESCRIPTION OF SERVICES (“SERVICE”)

Sirdata hosts, on one or more Servers, on behalf of the Client, one or more Server Containers named Google Tag Manager Server (hereinafter referred to as “sGTM”), provided by the third-party company Google (“Google”), hereinafter the “GTM Server hosting service”.

Sirdata is responsible for monitoring and maintaining the Server(s) and provides the Client with secure access to the Service Account via the URL: https://sgtm.sirdata.io.

The Client warrants that it shall use the Service in accordance with the public documentation provided by Sirdata, available at the following URL: https://server-side.docs.sirdata.net.

The Client manages the sGTM Server Container(s), Tags, and the processing of HTTP Requests and its Data through the interface provided by Google and accessible at: https://tagmanager.google.com.

The Client acknowledges that an sGTM Server Container is software developed by Google and that Sirdata acts solely as a hosting provider.

The Client further warrants that it shall use the Server and the sGTM Server Container in compliance with Google’s terms of use, available at https://policies.google.com/terms, Google’s privacy policy, available at https://policies.google.com/privacy, the Google Tag Manager use policy available at https://www.google.fr/tagmanager/use-policy.html, and the Google Tag Manager use policy available at https://marketingplatform.google.com/intl/fr/about/analytics/tag-manager/use-policy/.

For the purposes of the Service, the Client authorizes Sirdata to modify the headers of incoming HTTP Requests in order to add additional parameters, in particular:

(i) X-Appengine-Country: country of origin of the request, as an ISO 3166-1 alpha-2 country code, determined based on the IP address of the request origin.
(ii) X-Appengine-Region: region of origin of the request, as an ISO 3166-2 region code, determined based on the IP address of the request origin.
(iii) X-Appengine-City: city of origin of the request, determined based on the IP address of the request origin.
(iv) X-Appengine-User-IP: IP address of the request origin.
For the purposes of the Service, the Client authorizes Sirdata to modify the headers of incoming HTTP Requests in order to remove or replace headers when necessary, in particular (an asterisk “*” indicates any character string starting with the preceding characters):
(i) X-Forwarded-For: list of IP addresses separated by commas, including the original IP address of the request and the IP addresses through which the HTTP request was routed;
(ii) X-Forwarded-Proto: indicates “http” or “https” depending on the protocol used by the client to connect to the application;
(iii) X-*
(iv) Bunny*
(v) Via
(vi) Accept-Encoding
(vii) Connection
(viii) Keep-Alive
(ix) Proxy-Authorization
(x) TE
(xi) Trailer
(xii) Transfer-Encoding
For the purposes of the Service, the Client instructs Sirdata to modify the response headers to HTTP Requests in order to add, remove or replace parameters when necessary, in particular:

(i) Cache-Control, Pragma, Expires, and Vary (specify caching strategy)
(ii) Connection
(iii) Content-Encoding (compression method used, if any, for the response)
(iv) Content-Length
(v) Keep-Alive
(vi) Proxy-Authenticate
(vii) Server
(viii) Alt-Svc
(ix) Via
(x) Trailer
(xi) Transfer-Encoding
(xii) Upgrade
(xiii) Etag
(xiv) Age

Header	**Definition**	**Possible Values**	**Example**	**Activation by Default**
Gtm_config_id	sGTM configuration ID at Sirdata	string	2hDUjf	Yes
Gtm-Helper-Consent	Generic consent signal. Sirdata attempts to infer consent choices from available information (Google Consent Mode signals, TCF TC String, etc.)	true/false/undefined	false	Yes
Gtm-Helper-Consent-Analytics	Consent signal for audience measurement. Sirdata attempts to infer consent choices from available information (Google Consent Mode signals, TCF TC String, etc.)	true/false/undefined	false	Yes
Gtm-Helper-Consent-Basic-Ads	Consent signal for standard advertising. Sirdata attempts to infer consent choices from available information (Google Consent Mode signals, TCF TC String, etc.)	true/false/undefined	false	Yes
Gtm-Helper-Consent-Basic-Content	Consent signal for standard content. Sirdata attempts to infer consent choices from available information (Google Consent Mode signals, TCF TC String, etc.)	true/false/undefined	undefined	Yes
Gtm-Helper-Consent-Personalized-Ads	Consent signal for personalized advertising. Sirdata attempts to infer consent choices from available information (Google Consent Mode signals, TCF TC String, etc.)	true/false/undefined	false	Yes
Gtm-Helper-Consent-	Consent signal for personalized content. Sirdata attempts to infer consent choices from available	true/false/undefined	undefined	Yes

Header	Definition	Possible Values	Example	Activation by Default
Personalized-Content	information (Google Consent Mode signals, TCF TC String, etc.)			
Gtm-Helper-Cookieless-Id-Cross-Domain	Universal cookieless identifier (enables cross-site tracking). If the service is inactive or the specific DPA is not signed, the value will be "unsubscribed". If the user has not given consent, the value will be "no-consent". Otherwise, the value will be a UUID V4 user ID.	unsubscribed/no-consent/UUID V4	no-consent	No
Gtm-Helper-Cookieless-Id-Domain-Specific	Domain-specific cookieless identifier (does not enable cross-site tracking). If the service is inactive or the specific DPA is not signed, the value will be "unsubscribed". If the user has objected to processing, the value will be "objected". Otherwise, the value will be a UUID V4 user ID.	unsubscribed/objected/UUID V4	f577fc8e-065a-5e5f-6008-eacbc29c17de	No
Gtm-Helper-Device-Is-Mobile	Type of mobile device (true/false)	true/false/undefined	false	Yes
Gtm-Helper-Device-User-Agent	Device user-agent (not pseudonymized if proxyfication is enabled; the User-Agent sent to GA4 is pseudonymized)	string	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36	Yes
Gtm-Helper-Optout	Opt-out signal. Sirdata infers the opt-out signal from the "gtm-helper-optout" cookie with a non-null value (e.g., "true", "1") which must be set on the host used for sGTM (e.g., "tag.example.com") or the domain prefixed by a dot (e.g., ".example.com")	true/false/undefined	undefined	Yes
Gtm-Helper-Site-Domain	Domain from which the request originates	string	alertepv.com	Yes
Gtm-Helper-Site-Host	Host from which the request originates	string	www.alertepv.com	Yes
Gtm-Helper-Site-Origin	Origin of the request	string	www.alertepv.com	Yes
Gtm-Helper-User-City	User's connection city	string	Paris	Yes

Header	Definition	Possible Values	Example	Activation by Default
Gtm-Helper-User-Country	User's connection country	ISO 3166-1 alpha-2 country code	FR	Yes
Gtm-Helper-User-Ip	User's IP address (not truncated if proxyfication is enabled; IP sent to GA4 is truncated)	IP address	1.1.1.1	Yes
Gtm-Helper-User-Isp	Internet service provider or VPN (e.g., Apple's "Privacy Relay")	string	Free Pro SAS	Yes
Gtm-Helper-User-Region	User's connection region	ISO 3166-2 region code	IDF	Yes

As part of the use of the Service, the Client acknowledges that it may activate the Advanced Data Enrichment Offer via GTM Helper in its Service Account.

The Client agrees that upon activation of the Advanced Data Enrichment Offer via GTM Helper in its Service Account, Sirdata is expressly authorized to intervene in relation to the Data, including but not limited to the headers of incoming HTTP Requests, in accordance with Annex 2.

Sirdata reserves the exclusive right, at its discretion, to modify, add or delete any parameter in the headers of incoming HTTP Requests based on its operational, strategic, and technical requirements, including but not limited to those described in the following table:

As part of the use of the Service and subject to the activation of the Advanced GTM Helper Option, the Client expressly authorizes Sirdata to block “Set-Cookie” directives in requests in order to prevent the placement of cookies in the absence of a valid consent signal.

Sirdata reserves the exclusive right to adapt or evolve these processes based on operational or technical constraints, or legal requirements, without prior notice to the Client.

The Parties agree that the operational terms may be unilaterally modified by Sirdata, and their updated version will be regularly available in the documentation at the following URLs:

(i) https://server-side.docs.sirdata.net/sirdata-server-side/traitement-des-donnees/hebergement-seul

(ii) https://server-side.docs.sirdata.net/sirdata-server-side/traitement-des-donnees/surcouche-gtm-helper

ANNEX 2 – PERSONAL DATA PROCESSING – DATA PROCESSING AGREEMENT (DPA)

The Controller and the Processor acknowledge the need to base their relationship on principles of transparency, openness, and cooperation in order to ensure compliance with the Applicable Data Protection Regulation in the context of the Service provided by the Processor.

The Processor represents and warrants that it offers the Service in compliance with the obligations incumbent upon it under the Applicable Data Protection Regulation.

To this end, the Processor undertakes to provide the Controller with appropriate safeguards regarding the implementation of technical and organizational measures so that the processing of Personal Data it performs under the GTCS complies with the requirements of the Applicable Data Protection Regulation and ensures the rights of the Data Subjects.

I – Compliance with Instructions

The Processor shall process Personal Data, including those generated in connection with the Service, solely on behalf of and in accordance with the documented instructions of the Controller within the scope of the Service. Said Personal Data shall not be subject to any processing operation other than those necessary for the provision of the Service, as described in particular in Annex 1.

If the Processor considers that an instruction from the Controller constitutes a violation of Applicable Data Protection Legislation or is likely to prevent the provision of the Service, the Processor shall immediately inform the Controller without delay, by email with acknowledgment of receipt addressed to the person who gave such instruction.

The Personal Data, including the Personal Data generated in connection with the Service, may not be used by the Processor for its own purposes or for those of another client or service provider. The Processor also undertakes not to make any copy, whether full or partial, of the Personal Data without the Controller's prior written consent, except for copies strictly necessary for the performance of the GTC and for the provision and invoicing of the Service.

II – Subprocessing

The Processor may engage another processor (hereinafter the "**Sub-Processor**") to carry out specific processing activities. In such cases, the Processor shall provide the Controller with prior written notice of any intended changes concerning the addition or replacement of Sub-Processors.

This information must explicitly indicate the subcontracted processing activities, the identity and contact details of the Sub-Processor, and the dates of the subcontracting agreement.

The Controller shall have a minimum period of one (1) month from the date of receipt of this information to raise any objections. Such subcontracting may only proceed if the Controller has not objected within the agreed time period.

The Sub-Processor shall be required to comply with the obligations of these GTCS on behalf of and in accordance with the instructions of the Controller. It is the responsibility of the initial Processor to ensure that the Sub-Processor provides sufficient guarantees regarding the implementation of appropriate technical and organizational measures to meet the requirements of applicable data protection law. Where the Sub-Processor fails to fulfill its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of the Sub-Processor's obligations.

The Processor declares, as of the date of signature of the GTC, that it uses the following Sub-Processors:

Name	Address	Type of Service	Location	Personal Data Processing
AWS	38 Avenue John Kennedy, Luxembourg, Luxembourg	Hosting	EU	Yes
Cloudflare	101 Townsend St, San Francisco, CA 94107, United States	Content Delivery Network, DNS	Global	Yes
Bunny	BunnyWay d.o.o., Cesta komandanta Staneta 4A, 1215 Medvode, Slovenia	Content Delivery Network, DNS	Global	Yes
Scaleway	8 rue de la Ville l'Évêque, 75008 Paris, France	Web Hosting	Global	Yes
Hetzner	Industriestr. 25, 91710 Gunzenhausen, Germany	Web Hosting	Global	Yes
Google Cloud France (GCP)	8 Rue de Londres, 75009 Paris, France	Web Hosting	Global	Yes

III – Security

The Processor undertakes to implement all appropriate technical and organizational measures to ensure the confidentiality, security, and integrity of Personal Data, notably to prevent any unauthorized access, use or disclosure, and to protect the Personal Data collected and processed under the performance of the GTCS against any alteration, destruction or accidental or unlawful loss.

The security measures specifically include, at a minimum, the objectives and/or security measures set forth in Annex 5.

The Processor shall:

(i) Process Personal Data separately from its own data or that of its other clients;
(ii) Store Personal Data in encrypted storage spaces accessible via complex passwords;
(iii) Restrict access to Personal Data exclusively to persons authorized and specifically empowered by the Processor who require access to such data for the purpose of providing the Service;
(iv) Ensure that persons authorized to access Personal Data under the GTCS commit to confidentiality or are subject to an appropriate legal obligation of confidentiality and receive the necessary training regarding personal data protection;
(v) Establish mechanisms to restore the availability of and access to Personal Data within appropriate timeframes in the event of a physical or technical incident;

(vi) Implement procedures aimed at regularly testing, analyzing, and assessing the effectiveness of technical and organizational measures to ensure the security of Personal Data processing;

(vii) Incorporate data protection principles by design and by default into its tools, products, applications, or services.

IV - Notification of Personal Data Breaches

In the event of a Personal Data Breach, the Processor shall take appropriate corrective measures to stop the identified breach and protect the affected Personal Data.

The Processor shall notify the Controller of any Personal Data Breach as soon as possible and no later than forty-eight (48) hours after becoming aware of it. Such notification shall be accompanied by all useful documentation to enable the Controller, if necessary, to notify the competent Supervisory Authority.

The Processor shall provide the Controller, free of charge and in writing, with the following elements:

(i) The nature of the Personal Data Breach, including, if possible, the categories and approximate number of Users affected by the breach;

(ii) The name and contact details of the Data Protection Officer or any other point of contact from whom additional information can be obtained;

(iii) The probable consequences of the Personal Data Breach;

(iv) The measures taken or proposed by the Processor to address the Personal Data Breach.

Where and insofar as it is not possible to provide the information simultaneously, the information may be provided in phases without undue delay, specifying the reasons for such delay.

V - Transfer of Personal Data outside the European Union

Personal Data processed by the Controller are processed and hosted by the Processor within the territory of the European Union.

Pursuant to Article 46 of the GDPR, Personal Data may be transferred to a third country providing an adequate level of protection as recognized by the European Commission or provided that Appropriate Safeguards are implemented in compliance with Applicable Data Protection Legislation to secure the transfer of Personal Data. The Processor shall not be liable for the consequences arising from legislative modifications or new interpretations from Supervisory Authorities occurring after the signature of these GTCS, provided it has implemented adequate measures complying with Articles 44 to 49 of the GDPR as of the date of said transfer.

The Processor shall use reasonable efforts to avoid transferring Personal Data outside the European Union ("**EU**").

Nevertheless, such transfer may be carried out if strictly necessary for the performance of services under these GTCS, in accordance with Article 6(1)(b) of the GDPR, which allows processing of Personal Data essential for the proper performance of a contract to which the data subject is party.

Moreover, if operationally or technically required, the transfer may take place subject to implementing Appropriate Safeguards in compliance with applicable legal requirements, and the Processor undertakes to inform the Controller thereof. Explicit written authorization from the Controller shall be required solely for transfers not covered by standard safeguards (hosting, backup, maintenance, administration, helpdesk, etc.).
Appropriate Safeguards refer to all legal, technical, and organizational mechanisms implemented by the Processor or any other entity involved in processing Personal Data to ensure protection levels compliant with GDPR requirements, notably regarding transfers to third countries.

These Appropriate Safeguards include, without limitation:

(i) Standard Contractual Clauses adopted by the European Commission;
(ii) Binding Corporate Rules (BCR);
(iii) Recognized certification mechanisms, approved Codes of Conduct, or any other legal instrument acknowledged by competent authorities to safeguard Personal Data transferred outside the EU, in accordance with Articles 46 to 49 of the GDPR.

The Controller acknowledges that engaging sub-processors such as AWS, Google Cloud, or other cloud service providers does not automatically entail data transfers outside the EU unless interpreted otherwise by Supervisory Authorities. In such case, Sirdata cannot be held liable provided Appropriate Safeguards as defined in the GDPR are in place at the time of processing.

In case of a request to transfer data outside the EU, the Processor shall implement Appropriate Safeguards within operational and technical constraints to ensure transfer compliance with the GDPR.

Exceptionally, when safeguards under Article 46 cannot be implemented or absent an adequacy decision ensuring an equivalent protection level, a Personal Data transfer outside the EU may still be carried out pursuant to derogations listed in Article 49 of the GDPR, including, among others:

(i) Explicit consent of the data subject to the proposed transfer, having been informed of possible risks associated in the absence of adequate safeguards;
(ii) Transfers necessary for performance of a contract between the data subject and the Controller, or pre-contractual measures requested by the data subject;
(iii) Transfers necessary for establishing, exercising, or defending legal claims;
(iv) Transfers necessary for important reasons of public interest.

The Processor shall obtain written authorization from the Controller whenever relying on derogations under Article 49 to transfer Personal Data outside the EU.

The Controller acknowledges a Supervisory Authority may interpret that data processed through infrastructure provided by a cloud or *content delivery network* ("CDN") service provider constitutes a transfer under GDPR, including when processing occurs within the EU.

The Controller expressly accepts these transfers in advance, provided Appropriate Safeguards defined by Articles 44 to 49 of the GDPR are in place. Explicit written authorization from the Controller shall be required only for transfers not covered by these safeguards. The Controller further agrees to bear full responsibility for the consequences thereof and to hold Sirdata harmless from any liability or claims linked to such transfer, including, without limitation, subcontractors such as AWS, Google Cloud, and Cloudflare.

This clause also covers circumstances where legislative amendments or interpretations by Supervisory Authorities impose new data transfer obligations regarding data transfer. Sirdata, as Processor, cannot be held liable provided it implemented Appropriate Safeguards under Articles 44 to 49 of the GDPR to protect Personal Data.

VI – Cooperation

The Processor undertakes to:

(i) Respond diligently and in writing to any information requests from the Controller within fifteen (15) business days from receipt of the request, enabling the Controller to address requests for exercising rights of access, rectification, erasure, or objection, the right to restriction of processing, data portability, and/or the right not to be subject to automated individual decision-making (including profiling) submitted by Users or any other individuals whose data is processed in connection with the use of Websites published by the Controller, as well as requests from supervisory authorities, the Controller's auditors, or the Controller's Data Protection Officer. The Processor shall also ensure this period does not exceed 30 days, in accordance with GDPR requirements, except under exceptional circumstances.

(ii) Immediately forward to the Controller any request from a User or other data subject related to Personal Data processing. Such forwarding must occur promptly upon receiving the request, so as not to delay the exercise of the rights of data subjects.

(iii) Assist the Controller in conducting data protection impact assessments and, if applicable, prior consultation with the Supervisory Authority. The Processor shall provide all necessary information regarding the technical infrastructure and security measures implemented, allowing for a comprehensive assessment of risks associated with Personal Data processing.

(iv) Generally make available to the Controller all necessary documentation to demonstrate compliance with all its obligations. This documentation must include audit reports, data security policies, and any other evidence demonstrating the Processor's compliance with its legal and contractual obligations.

VII – Duration of the Personal Data conservation

Personal Data shall be retained for the period strictly necessary for the provision and proper functioning of the Service, in accordance with the purposes set out in the GTCS. The Processor undertakes to comply with the retention periods determined by the Controller, in accordance with applicable legal requirements, in particular Article 5(e) of the GDPR, which provides that personal data shall not be kept for longer than is necessary.

Pursuant to the GTCS and unless expressly requested by the Controller to return the data, the Processor undertakes to irreversibly destroy all Personal Data processed in connection with the Service. Such destruction must ensure that the data cannot be recovered, in accordance with Article 28(3)(g) of the GDPR.

The Processor shall provide the Controller with a written certificate confirming the effective destruction of the Personal Data within five (5) days of such destruction. This certificate shall specify the methods used to destroy the data and confirm that all data has been deleted in accordance with applicable security standards.

VIII - Liability and Remedies

1. **Obligations of the Controller**

The Controller undertakes to provide the Processor with clear, complete instructions compliant with the General Data Protection Regulation (GDPR) and all other applicable data protection laws. The Controller also guarantees the legality of collecting the Personal Data entrusted to the Processor and commits to active cooperation with the Processor to fulfill regulatory and contractual obligations.

2. **Liability of the Controller**

In the event of fault, negligence, or breach of data protection obligations attributable to the Controller, the Controller shall be held liable for any direct or indirect harm suffered by the Processor, including penalties, fines, or damages imposed on the Processor due to inaccuracies in instructions, lack of cooperation, or any other failure related to GDPR compliance.

3. Recourse of the Processor

The Processor may seek recourse against the Controller and claim compensation in the event of damage caused by a breach of the Controller's obligations, as defined in these General Terms and Conditions of Sale and under applicable laws. The Processor may, in particular, claim:

(i) Reimbursement of fines or financial penalties imposed by a data protection authority as a result of the Controller's breaches;
(ii) Compensation for financial losses related to service interruptions, reputational harm, or loss of business opportunities resulting from the Controller's wrongful acts or omissions.

4. Limits of the recourse

Any claim or recourse by the Processor against the Controller must be submitted in writing within thirty (30) business days following discovery of the event causing the damage. The total amount of compensation due from the Controller shall not exceed the total amounts paid by the Controller to the Processor for the current contractual period, except in cases of gross negligence or intentional misconduct.

5. Cooperation and Joint Defense

In the event of a claim from a supervisory authority or third party regarding a Personal Data breach, the Parties agree to actively cooperate in defending their respective interests. If one Party is required to pay a sum to a third party due to a breach attributable to the other Party, the Party may seek reimbursement of sums paid, including reasonable legal defense fees.

VIII – Audit

The Controller reserves the right, at its sole expense, to carry out any verification it deems useful to ascertain the Processor's compliance with its obligations under the General Terms and Conditions of Sale, including through audits. This right includes both regular and ad hoc verifications, as needed by the Controller, to ensure that the processing of Personal Data complies with legal and contractual requirements.

The Processor undertakes to comply with the Controller's audit requests, whether conducted directly by the Controller or by a trusted third party selected by the Controller, acting as an independent auditor with appropriate qualifications and free to report all audit findings and observations directly to the Controller.

The Controller shall notify the Processor in writing of any audit request with at least fifteen (15) days' prior notice. The audit must be conducted in a manner that minimizes disruption to the Processor's business activities. The Parties shall actively cooperate to define the specific conditions of the audit, including the timing and methodology to be applied.

Following the audit, the Processor shall receive a copy of the audit report and shall implement any necessary corrective measures within a reasonable timeframe if any non-compliance or deficiencies are identified. The costs of such compliance measures shall be borne by the Processor only where the measures are required to meet a legal obligation.

IX - Data Protection Officer (DPO)

The Processor shall provide the Controller with the name and contact details of its Data Protection Officer: Naïma CONTON - nco@sirdata.fr.

X - Records of categories of processing activities

The Processor undertakes to maintain and make available a record of the processing of Personal Data carried out on behalf of the Controller, which shall include:

(i) The name and contact details of the Controller and the Data Protection Officer;

(ii) A description of the categories of Data Subjects affected by the Processing and the categories of Personal Data subject to the Processing;

(iii) The categories of recipients to whom the Personal Data have been or will be disclosed, including recipients located outside the European Union;

(iv) Where applicable, the legal basis and appropriate safeguards for Transfers of Personal Data to a country of the European Union, including identification of the country concerned;

(v) The envisaged retention periods for the erasure of the various categories of Personal Data, in accordance with applicable legal requirements;

(vi) A general description of the technical and organizational security measures implemented to ensure the confidentiality, integrity, and availability of the Personal Data, in accordance with Article 32 of the GDPR.

ANNEX 3: PRICING

The prices referred to in this appendix are indicated in euros and excluding applicable taxes or duties, which are the responsibility of the Customer.

I- Installation costs

Each installation of a Server Container will be billed at €500 excluding tax.

II- Amount invoiced for the Service

The Service is billed based on the number of HTTP requests routed to all of the Client's Server Containers ("**Hits**"), with or without Data Enrichment.

In the event of a dispute between the Parties on the basis of invoicing, the data, statistics and data volumes recorded in Sirdata's information systems will be authentic and will be considered irrefutable, thus constituting the sole basis for final invoicing as accurate by the Parties and will constitute the basis on which final invoicing will be based.

The fixed and variable amounts will be adjusted according to the monthly Hits range, according to the grid below. Sirdata reserves the right to modify the pricing conditions after notification to the Customer under the conditions stipulated in these General Terms and Conditions.

Monthly range of Hits		Fixed amount	Variable amount (“overrun”)
From...	To...		By tranche of 100 000 Hits
0	2,000,000	89 €HT	-
2,000,001	5,000,000	89 €HT	1.99 €HT
5,000,001	10,000,000	139 €HT	1.79 €HT
10,000,001	25,000,000	189 €HT	1.59 €HT
25,000,001	50,000,000	389 €HT	1.49 €HT

50,000,001	75,000,000	739 €HT	1.44 €HT
75,000,001	100,000,000	989 €HT	1.39 €HT
100,000,001	150,000,000	1 289 €HT	1.34 €HT
150,000,001	∞	1 889 €HT	1.29 €HT

Exemples:

(i) For 1,300,000 Hits routed to a Server Container during the month, the amount invoiced will be €89 excluding tax;

(ii) For 4,230,000 Hits routed to a Server Container in the month, the amount billed will be €133.38 excluding tax, i.e. a fixed amount of €89 excluding tax and €44.38 excluding tax (22.3*€1.99 excluding tax) for excess;

(iii) For 14,180,000 Hits routed to a Server Container in the month, the amount billed will be €255.46 excluding tax, i.e. a fixed amount of €189 excluding tax and €66.46 excluding tax (41.8*€1.59 excluding tax) for excess.

In certain cases, the Customer can activate and manage their service directly via the marketplace of a “cloud” service provider, such as AWS or Google Cloud. In this case, billing will be handled by the cloud service provider. Sirdata cannot be held responsible for billing terms or potential errors induced by the service provider “*cloud*". Billing will be entirely covered by the cloud service provider, according to their own conditions.

The first Server Container is included in the service price. Each active Server Container beyond the first will result in monthly billing of €29 excluding tax.

III – Professional Services

For the purposes of these GTCS, the seniority levels of personnel and hourly rates invoiced are defined as follows:

Seniority Level	***Hourly Rate invoiced for professional services (€ excl. taxes)***
Junior: Less than two (2) years of experience	*€190 per hour*
Intermediate: Between two (2) and five (5) years of experience	*€280 per hour*
Senior: More than five (5) years of experience	*€420 per hour*
Partner: Partner with over ten (10) years of experience	*€600 per hour*

ANNEX 4: SERVICE LEVEL AGREEMENT ("SLA")

1) Availability of the User Interface

Sirdata undertakes to implement the necessary measures to ensure the availability of the user interface and hosted services at a level of **99%** on a monthly basis. However, this availability excludes scheduled maintenance periods, incidents due to force majeure events, or interruptions caused by external factors beyond Sirdata's control (such as network failures, third-party infrastructure issues, or actions by the Client).

Service availability is measured monthly and calculated using the following formula:

$$\text{Availability (\%)} = \left(\frac{\text{Total Time} - \text{Downtime}}{\text{Total Time}} \right) \times 100$$

Where:

- **Total Time** represents the total number of hours in the month (generally 24h × number of days in the month).

- **Downtime** refers to the total duration (in hours) during which the service was unavailable due to unplanned incidents, excluding scheduled maintenance periods, force majeure, or external factors not attributable to Sirdata (e.g., network failures, third-party infrastructures, or Client's actions). Interruptions caused by third parties, anomalies arising from external providers, or Client actions or omissions are not included in availability calculations.

Scheduled maintenance will be communicated to the Client at least seven (7) days in advance and conducted outside regular business hours (between 11:00 PM and 6:00 AM).

2) Response Times and Performance

Sirdata guarantees an average response time of its user interface of 5 seconds for any User located in France. Sirdata will use reasonable efforts to maintain an average response time of less than 5 seconds for access and navigation within the user interface for Users located in metropolitan France. This response time is an average under normal conditions and does not constitute a strict guarantee.

In case of performance degradation, Sirdata will attempt to diagnose the cause within the timeframes detailed below and propose corrective actions, if technically feasible:

	Diagnosis / Response Time	**Workaround**	**Correction**
Blocking Anomaly	6 hours	1 day	3 days
Major Anomaly	12 hours	3 days	7 days
Minor Anomaly	3 days	14 days	28 days

Sirdata cannot be held responsible for performance degradations due to external factors (e.g., internet network issues, third-party providers).

The deadlines mentioned in this SLA are indicative and may vary depending on technical constraints, resource availability, and incident severity. Sirdata will strive to comply with these deadlines as far as reasonably possible but cannot guarantee compliance in all circumstances. In the event of exceeding these deadlines, Sirdata undertakes to inform the Client promptly and provide regular updates on corrective actions.

3) Anomaly Management

Sirdata commits to adhering to the following indicative intervention and correction times. Anomalies will be categorized into three levels with indicative deadlines for diagnosis, workaround solution, and correction, subject to available resources and technical constraints:

- **Blocking Anomaly**: Complete service interruption affecting all users. All requests return an HTTP error code 429 (Too Many Requests), 500 (Internal Server Error), 502 (Bad Gateway), 503 (Service Unavailable), or 504 (Gateway Timeout) not attributable to the Client, or require loading times exceeding 5 seconds.

- **Major Anomaly**: Malfunction affecting a significant part of services. More than 5% of requests return HTTP error codes (429, 500, 502, 503, or 504) not attributable to the Client, or require loading times exceeding 5 seconds.

- **Minor Anomaly**: Minor defect with no major impact on operations.

4) Service Credits

To be eligible for Service Credits, the Client must notify Sirdata of the incident within 24 hours from detection, provide sufficient verifiable evidence, and obtain acknowledgment from Sirdata that the incident falls under its responsibility.

Interruptions caused by third-party providers, external network problems, or Client actions do not entitle the Client to Service Credits.

Service Credits for the sGTM product are defined in Sirdata's General SLA published on its website and calculated as described therein, including availability ranges and applicable caps. In the event of discrepancies, provisions of the General SLA shall prevail.

Service Credits are calculated based on actual availability as follows:

- Availability ≥ 99% : No credit;
- Availability between 95% and 99%: 10% credit of the monthly invoice;
- Availability between 90% and 95%: 25% credit of the monthly invoice;
- Availability < 90%: 50% credit of the monthly invoice.

Any claim for Service Credits must be notified by the Client within 15 days following the acknowledgment of the incident by Sirdata ("**Recognition**"). Recognition refers to Sirdata's express and written approval of the reported downtime following thorough analysis. Such recognition will only be granted after Sirdata completes a comprehensive assessment, including evaluation of Client-provided information, logs, and relevant technical data. Lack of response from Sirdata to a downtime notification shall not constitute implicit acknowledgment thereof.

The total amount of Service Credits shall be capped at 10% of the Client's total annual invoice for the concerned services, for all combined Service Credits in one year.

Service Credits shall be settled, invoiced, and paid within thirty (30) days following Sirdata's acknowledgment of the Anomaly.

5) Incident Notification and Management Process

(i) **Incident Reporting:** Only incidents reported within 24 hours after detection will be eligible for Service Credits. Detection is defined as the moment the Client becomes aware of the incident through monitoring tools, automated alerts, or manual observation. Exceptions may apply if the Client demonstrates, with supporting evidence, that notification delay was due to circumstances beyond reasonable control, such as force majeure, unexpected technical failures, or third-party disruptions.

The notification must include sufficient verifiable evidence (e.g., technical logs, screenshots, detailed anomaly descriptions) and necessary information enabling Sirdata to diagnose and validate the incident.

(ii) **Follow-up:** Sirdata shall inform the Client of the progress of major or blocking incidents only if recognized as such by Sirdata. Updates will be provided based on Sirdata's technical availability and priorities.

(iii) **Reports:** Incident reports will be provided only upon Client request, subject to additional charges as defined in Annex 3 – Professional Services.

6) Exceptions and Exclusions

Sirdata's obligations do not apply in the following cases:

(i) Scheduled maintenance interventions, notified to the Client at least 7 days in advance.
(ii) Interruptions due to actions or omissions by the Client or its subcontractors.
(iii) Issues related to third-party software not provided by Sirdata.
(iv) Force majeure events as defined in Article [XX] of the GTCS (e.g., natural disasters, war, labor disputes, strikes, pandemics, etc.).
(v) Interruptions due to failures of networks external to Sirdata, such as global internet networks or Client access infrastructures.
(vi) Limited recourse in case of SLA breach.
(vii) Force majeure events as defined in the main GTCS (natural disasters, strikes, pandemics, etc.).

In case of non-compliance with SLA commitments by Sirdata, the Client may request early termination of the GTCS only after sending formal notice to Sirdata and allowing Sirdata a minimum period of 60 days to rectify identified breaches. Any penalty or early termination claim must be justified and validated by Sirdata.

This SLA exclusively applies to the sGTM product and supplements Sirdata's General SLA. In case of discrepancy, provisions of the General SLA shall prevail unless expressly stated otherwise in this SLA.

ANNEX 5: INFORMATION SYSTEMS SECURITY MEASURES

1. Awareness and Team Training

a. Awareness training on best practices related to information systems security and personal data protection
b. Implementation of an IT usage policy
c. Implementation of security and confidentiality contractual clauses with partners and clients
d. Data management protocols according to processing activities and the roles of Sirdata's staff members

2. Knowledge of Information Systems

a. Comprehensive mapping of the network and inventory of critical assets
b. Inventory of privileged accounts
c. Procedures governing onboarding and offboarding based on user roles
d. Procedures for managing network connections

3. Authentication and Access Control

a. Account management policy / Access registry
b. Account activity logging and system monitoring and alerting procedures
c. Password management policy, including complexity requirements
d. Procedures to secure passwords stored within systems

4. Endpoint Security

a. Implementation of minimum-security standards across all IT devices (firewalls, automatic session locking, etc.)
b. Minimum security standards across all IT equipment, with automatic backups outsourced via Google Cloud, Online
c. Protocol protecting against threats from removable media use
d. Firewall activation and configuration
e. Cloud-based infrastructure; computer networks, infrastructures, and systems accessible exclusively by authorized personnel
f. Network segmentation and separation of zones
i. No DMZ; use of Kubernetes cluster

5. Network Security

a. Security protocols for Wi-Fi access networks and usage separation
i. Dedicated Sirdata Wi-Fi via Orange fiber for employees
ii. Guest network via VDSL OVH for external users
b. Secure access protocols
i. TLS used for all outbound internet traffic
c. Secure access gateway
d. Protection protocol for professional email communications
e. Secure protocol for dedicated partner interconnections
i. Encrypted APIs only
ii. Encryption of all inbound and outbound connections
f. Control and protection of server rooms

6. Administrative Security

a. Verification procedures for endpoints and servers conducted by administrators
b. Administrative rights management protocols restricted strictly to operational needs
c. Dedicated and isolated network for IT system administration
i. Limited to two persons with encrypted/secured workstations
ii. Completely isolated from general office networks

7. Protocols for Mobile Working (Nomadism)

a. Implementation of two-factor authentication
b. Access to intra-cluster services via OpenVPN
c. Physical security measures for mobile terminals
i. Unmanaged computers; access to user accounts managed remotely by admins, subject to dual encryption on devices and their accesses
d. Network connection security for devices used remotely
i. Access to intra-cluster services via OpenVPN

8. Information Systems Maintenance

a. Automated security updates and use of Linux distribution packages

9. Monitoring, Auditing, and Incident Response Procedures

a. Regular data restoration drills
b. Dedicated individual responsible for server infrastructure security, authorizations, and service access control

10. Data Lifecycle Management Protocols

a. Designation of a single contact for data reception when transfers are not machine-to-machine
b. Data retention policy specifying storage duration for processed personal data
c. Protocol governing access to archived data
d. Data classification policy and control measures
e. Processing of personal data exclusively within the European Economic Area
f. Utilization of recognized encryption protocols and algorithms: OpenSSL, AES-512, ECDSA, Let's Encrypt, Certbot, OpenVPN, RSA
g. Use of encrypted keys stored within keychains on encrypted disks
h. Paper document management protocol integrated into personal data lifecycle management procedures

11. Supervision of Software Development

a. Implementation of procedures governing user privacy and access (implementation of a Consent Management Platform—CMP—across our entire network, availability of privacy policies, and employee personal data management protocols)

12. Premises Security

a. Installation of log monitoring software (Logwatch and OSSEC).
b. Security protocols defining rules and methods for access control

13. Anticipation of Information Systems Capacity

a. Maintaining a service availability rate of 99%

14. Compliance with Legal Requirements

a. Implementation of a privacy policy and procedures to handle users' requests to exercise their rights in order to:

i. Allow users to apply their rights, including the right to rectify or amend their personal data

ii. Allow users to exercise their rights and/or make electronic requests concerning their personal data (e.g., requests for objection, modification, deletion)

iii. Display a deterrent warning message to any unauthorized individual attempting to access information system assets