**SONARQUBE SERVER TERMS AND CONDITIONS**

Last updated August 19, 2024

This Agreement is entered into by and between SonarSource and Customer to govern Customer's installation and use of SonarQube Server Products and related Support.

## 1. DEFINITIONS

1. "**Active Version**" means (i) the most recent version of the Product; (ii) the version preceding the most recent version of the Product; (iii) the most recent LTA version of the Product; or (iv) the LTA version preceding the most recent LTA version of the Product, but only for a 6-month period after the most recent LTA version is released.
2. "**Agreement**" means these SonarQube Server Terms and Conditions.
3. **"Authorized Contact(s)"** means the person or group of people Customer designates to contact SonarSource for Support.
4. "**Authorized Use**" means Customer's installation and operation of a Product to analyze code on each SonarQube Server Instance for which it has obtained a License Key.
5. "**Customer**" means the entity that has purchased a License for a Product or Support, or who will be using the License in accordance with their Authorized use. The term "Customer" when interpreting the scope of a License or Authorized Use includes affiliates of Customer, as well as any persons granted access to a Product by Customer or its affiliates for their Authorized Use.
6. "**Commencement Date**" means the date that SonarSource sends a License Key to Customer.
7. "**Community Edition**" means the open-source SonarQube Server and SonarLint software that is available free of charge under a GNU Lesser GPL license (Version 3) via the Website. The Community Edition is not covered by this Agreement.
8. "**Data Processing Addendum**" means the SonarSource data processing addendum referenced in Section 6 and attached hereto.
9. "**Documentation**" means the official user documentation prepared and provided by SonarSource to Customer on the use of the Products (as updated from time to time). For the avoidance of doubt, any online community site, unofficial documentation, videos, white papers, related media, or feedback do not constitute Documentation.
10. "**Intellectual Property**" means all present and future intellectual and industrial property rights, whether obtained or conferred by registration, automatically, by statute, by common law or in equity; and wherever existing or created.
11. "**License**" means a license for Customer to use a Product for an approved SonarQube Server Instance for a set period of time from the Commencement Date, subject to this Agreement.
12. **"License Key"** means the key that SonarSource provides to activate the Product for a specified period of time on a specified SonarQube Server Instance in accordance with its License.
13. "**Lines of Code**" means the addition of the lines of code for each project analyzed in a SonarQube Server Instance. The lines of code of a project are found by the SonarQube Server software during the analysis of a project by counting the lines of code of the largest branch analyzed for that project. They are not cumulative when the same project is re-analyzed.
14. "**LTA**" means the then-current long-term Active Version of a Product, as described on the Website.
15. "**Party**" means SonarSource or Customer individually, and "**Parties**" means SonarSource and Customer together.
16. "**Personal Data**" means any information relating to an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information", or similar terms as defined in applicable data protection law.
17. "**Product**" means a commercial edition of the SonarQube Server software that SonarSource offers for a fee, as listed on the Website. The Community Edition is not a Product under this definition.
18. "**SonarQube Server Instance**" means the server that Customer identifies to be licensed under this Agreement.
19. "**SonarSource**" means SonarSource SA, a Swiss company registered in Switzerland under UID No. CHE-114.587.664 with a mailing address of P.O. Box 765, CH-1215, Geneva 15, Switzerland.
20. "**Support**" means access to SonarSource's online support offering, as described on the Website.
21. "**Updates**" means all new features, improvements, or bug fixes that are provided for a Product.
22. "**Website**" means SonarSource's website at www.sonarsource.com and its sub-domain webpages.

## 2. PRODUCT EVALUATION

Customer may request a temporary License Key to evaluate a Product for a trial period prior to purchasing. SonarSource may accept or decline such a request at its own discretion.

## 3. SUPPORT

If Customer has purchased Support or is otherwise entitled to receive Support based on the License that Customer has purchased, SonarSource will provide Support in accordance with the Support terms attached hereto and set forth on the following page of the Website: https://www.sonarsource.com/legal/support-terms/. In order to receive Support, Customer must operate an Active Version of the Product.

## 4. DELIVERY AND PAYMENT

(a) Promptly following Customer's purchase of a License, SonarSource will provide Customer with a License Key.

(b) SonarSource will generally invoice Customer at the time it provides a License Key. Customer shall pay undisputed invoices by an electronic funds transfer to be received in SonarSource's account within thirty (30) days of receipt unless the Parties have agreed otherwise in writing. If an invoice is not timely settled in full, SonarSource may, at its reasonable discretion:

(i) reserved;
(ii) reserved; and
(iii) terminate this Agreement for cause in accordance with Section 14.

(c) Reserved.

(d) If Customer purchases through an authorized reseller, then Section 4(b) and 4(c) will not apply and all payment, invoicing, and credit terms for the purchase will be as agreed between Customer and the authorized reseller.

## 5. INTELLECTUAL PROPERTY RIGHTS

(a) Subject to the terms, conditions, and limitations of this Agreement, SonarSource grants Customer a worldwide, non-exclusive, non-transferable, non-sublicensable and revocable License for (i) the Authorized Use of a Product on the SonarQube Server Instance for which the License was purchased, (ii) the testing, staging, and disaster recovery of a Product on a separate SonarQube Server Instance, (iii) the use of the information a SonarQube Server Instance generates about a project, while that project is active in the SonarQube Server Instance, and (iv) if purchased or included, the receipt by an Authorized Contact of Support for a qualifying Product. The License is limited to a maximum Lines of Code and an annual term. No rights, licenses or warranties are provided to any of SonarSource's Intellectual Property rights, save as are covered by the License to use any Products and receive any Support that are provided for by this Agreement. Customer undertakes to comply with and not to challenge or misuse any of SonarSource's Intellectual Property rights.

(b) SonarSource shall have the right to intervene to defend Customer and its officers, directors, and employees ("**Customer Parties**") against any third-party claim that a Product infringes or misappropriates a third-party's Intellectual Property right ("**IP Claim**"). SonarSource shall indemnify Customer Parties against any damages finally awarded to the third party making the IP Claim, and all penalties, fines, and reasonable third-party costs (including reasonable attorneys' fees) paid by Customer Parties to the extent arising out of an IP Claim (collectively, "**IP Losses**"). SonarSource's obligations under this Section 5(b) shall not apply to the extent an IP Claim is based on or arises from (i) a combination or use of a Product with hardware, software, or other materials not provided by SonarSource; (ii) the modification of a Product by anyone other than SonarSource or its authorized agents;
(iii) the use of a Product not in accordance with the Documentation or this Agreement; (iv) Customer's breach of this Agreement; or (v) a Customer Party's negligence, fraud, or willful misconduct. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

(c) In the event of an IP Claim, SonarSource shall be entitled, at its own expense and option, to either (i) procure the right for Customer to continue utilizing the Product features at issue; (ii) modify the Product to render the Product non-infringing; or (iii) replace the Product with an equally suitable, functionally equivalent, compatible, non-infringing product. SonarSource's obligation to defend and indemnify requires that (a) Customer give notice to SonarSource of any IP Claim immediately upon becoming aware of the same; (b) Customer give SonarSource the sole right to conduct the defense of any claim or action, or the negotiation of any settlement, in respect of an IP Claim and does not at any time admit liability or otherwise settle or compromise or attempt to settle or compromise the IP Claim except upon the express written instructions of SonarSource; and (c) Customer act in accordance with SonarSource's reasonable instructions and gives SonarSource assistance as it shall reasonably require in respect of the conduct of the defense, including the filing of all pleadings and other court processes and the provision of all relevant documents. Sections 5(b) and 5(c) set forth Customer's sole and exclusive remedy from SonarSource for any IP Claim.

## 6. PERSONAL INFORMATION

Customer may choose to disclose the name and work email address of certain of its employees in connection with this Agreement. Customer acknowledges that any Personal Data that Customer (or others acting on Customer's behalf) provide for the purpose of performance of this Agreement will be processed in accordance with the SonarSource Privacy Statement and the Data Processing Addendum.

## 7. CONFIDENTIALITY

"**Confidential Information**" means all non-public information, materials, documentation, or data, relating to a Party's business, which is disclosed by one Party ("**Discloser**"), or received by the other Party ("**Recipient**"), in connection with this Agreement, and which is clearly identified or marked as confidential or proprietary at the time of delivery to Recipient or which a reasonable person would understand to be confidential or proprietary. Recipient undertakes to (i) protect the confidentiality of the Confidential Information with at least the same degree of care as it applies to its own Confidential Information of a similar nature, but in no event less than a reasonable degree of care; (ii) only use Confidential Information for purposes consistent with its rights and obligations under this Agreement; (iii) not reverse engineer or decompile Confidential Information; and (iv) not disclose Confidential Information to any third-party other than its employees, consultants, vendors or advisors who have a need to know and who are bound by confidentiality and non-use obligations no less restrictive than those set forth herein. Confidential Information shall not include any information which: (a) Recipient already knew at the time of disclosure; (b) is generally available to the public or becomes publicly known through no wrongful act of Recipient; (c) Recipient received from a third-party who had a legal right to provide it; and/or (d) Recipient developed independently of any knowledge of or access to any of Discloser's Confidential Information. Either party may disclose Confidential Information if required by law or regulatory authorities, provided that, so far as it is lawful to do so, Recipient gives prompt notice to Discloser, so that Discloser may contest the requirement to provide such information. Upon Discloser's written request, Recipient will return or destroy all Confidential Information in Recipient's possession within thirty (30) days of the request. Recipient may retain a limited number of electronic copies of the Confidential Information to comply with applicable law, and as may be automatically created, maintained, and destroyed by its standard backup processes and systems. Recipient will remain bound by its confidentiality obligations for any copies retained. SonarSource recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which requires that certain information be released, despite being characterized as "confidential" by the vendor.

## 8. CUSTOMER'S OBLIGATIONS

(a) Customer shall at all times:

(i) ensure that only Customer's Authorized Contact requests Support and only for Customer's benefit;
(ii) ensure that all Products are used only as expressly permitted in this Agreement;
(iii) advise SonarSource in writing within thirty (30) calendar days if Customer becomes aware of any person's unauthorized use or distribution of a Product;
(iv) verify and take sole responsibility for ensuring that the version of any Product that it is using or intends to use is compatible with the SonarQube Server Instance it was obtained for;
(v) only use an unmodified version of a Product that was downloaded from the Website or from an authorized third party as indicated on the Website;
(vi) only use a License Key that was provided by SonarSource;
(vii) report the discovery of any violations of this Agreement to SonarSource in writing, within thirty (30) calendar days of discovering a violation;
(viii) prohibit, by appropriate measures, any unauthorized resale, access to, or use of any Product on any other SonarQube Server Instances than the one for which a License was obtained;
(ix) only use Products and Support in compliance with applicable law; and
(x) ensure its agents, employees, consultants and subcontractors comply with this Agreement, as applicable.

(b) Customer is responsible for its own use of Products and for verifying the absence of any viruses, spyware, or malicious programming in its own server environment.

(c) Customer must not:

(i) decompile, reverse engineer, disassemble, modify, adapt, create derivative works from, or otherwise attempt to derive such information from any Product;
(ii) sell, resell, sublicense, redistribute, reproduce, transmit, circulate, disseminate, translate, or reduce to or from any electronic medium or machine-readable form any Product, or any portion or derivative of a Product, whether in whole or in part;
(iii) vary or amend any Authorized Use;
(iv) publish, promote, broadcast, circulate or otherwise seek to make any commercial use of SonarSource's name, trade name, trademarks, service marks or logo, without SonarSource's prior written consent;
(v) whether through deliberate or negligent act or act of omission of its employees, consultants, or subcontractors or otherwise, resell, distribute, or cause the distribution of any Product to any third party other than for an Authorized Use, or use any Product on any SonarQube Server Instance other than the SonarQube Server Instance for which it was originally Licensed (in which case separate Products should be bought for those other SonarQube Server Instances);
(vi) use the Product to analyze code outside of its SonarQube Server Instance, which is not already analyzed in its SonarQube Server Instance;
(vii) use the information a SonarQube Server Instance generated about a project, unless that project is active in the SonarQube Server Instance;
(viii) use any Products that have been modified by anyone other than SonarSource or its authorized agents;
(ix) disclose, publish, or otherwise make publicly available any benchmark, comparative, or performance tests

or evaluations on the Product without the express written permission of Company;

(x) perform, or direct any third party to perform, any benchmark, comparative, or performance tests or evaluations on the Product for competitive advantage;

(xi) employ, use, or engage artificial intelligence technology that is not part of the Products to ingest, interpret, analyze, train on, or interact with the data provided by the Products, or to engage with the Products in any manner, without the prior written consent of SonarSource; or

(xii) enhance, augment, or improve data provided by the Products without the prior written consent of SonarSource.

**9. REPRESENTATIONS AND WARRANTIES**

SonarSource represents and warrants to the best of its knowledge and belief that the Products will substantially perform in accordance with the Documentation and do not contain any computer code that:

(a) is designed to disrupt, disable, harm, modify, spy on, delete or otherwise impede in any manner, including aesthetic disruptions or distortions, the operations of any of Customer's software, firmware, hardware, computer systems or networks (sometimes referred to as "viruses" or "worms");

(b) would disable the Products or Customer's systems or impair their operation based on the elapsing of time or for exceeding the maximum numbers of Lines of Code during the effective period of any License; or

(c) would permit SonarSource or any third party to access a Product or Customer's systems, whether or not to cause disablement or impairment (sometimes referred to as "trap doors," "access codes" or "back door" devices).

**10. DISCLAIMER**

Save as expressly provided otherwise in this Agreement and to the maximum extent permitted by applicable law:

(a) SonarSource warrants that the Products and Support will, for a period of sixty (60) days from the date of your receipt, perform substantially in accordance with Products and Support written materials accompanying it. Except as expressly set forth in the foregoing, all Products and Support are provided on an "as is" basis and on an "as available" basis without any warranties or representations, whether express or implied, oral, or written, of any kind or nature, including, but not limited to, any warranties of quality, performance, reliability, security, non-infringement, merchantability, or fitness for any particular purpose, and SonarSource expressly excludes any such warranties, representations or implications that a Product will be error-free, complete, operate without interruption, or operate correctly with any given product, system or specifications of Customer; and

(b) SonarSource makes no guarantee as to the availability of its Products and Support, and SonarSource shall not be responsible for any loss resulting from the loss or deletion of any data or information resulting from the use of any Products or Support, or any network or system outages, file corruptions, or for any other alleged consequences of having used any Products or Support.

**11. LIMITATION OF LIABILITY**

(a) Save for either Party's willful breach of this Agreement or gross negligence, or an infringement by either Party of the other Party's Intellectual Property, neither Party will be liable for any lost profits nor for any special, indirect, incidental, or consequential damages, costs, or expenses, regardless of the form of action, even if such Party is advised of the possibility of such damages in advance.

(b) Save for either Party's willful breach of this Agreement or gross negligence, an infringement by either Party of the other Party's Intellectual Property, or IP Losses under Section 5, in no event will SonarSource's aggregate liabilities under any claims arising out of this Agreement exceed the fees Customer paid under this Agreement within the previous twelve (12) months for the Product or Support giving rise to the claim. SonarSource's aggregate liabilities for IP Losses under Section 5 shall not exceed three times (3x) the fees Customer paid under this Agreement within the previous twelve (12) months for the Product giving rise to the IP Losses.

(c) The foregoing liability limitations shall apply to the maximum extent allowed by the governing law of this Agreement.

**12. LOGO RIGHT**

SonarSource may include Customer's name in a list of its customers in marketing materials and on the Website, together with the names and logos of other SonarSource customers to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. Customer may revoke the foregoing right at any time by submitting a written request via e-mail to: contact@sonarsource.com. SonarSource shall comply with such a termination or revocation request within twenty (20) business days from receipt of such notice.

**13. ASSIGNMENT**

(a) SonarSource and Customer may assign or transfer their rights and/or obligations under this Agreement to a purchaser of all or a substantial part of its assets or shares or as part of a corporate restructuring, in accordance with the provisions set forth at FAR 42.1204. In the event of such a permitted assignment by Customer:

(i) SonarSource must be notified, in writing, within ninety (90) days of such assignment;
(ii) the assignee must agree in writing to be bound by the terms and conditions of this Agreement; and
(iii) upon completion of such assignment, the assignor shall make no further use of any Products or Support under this Agreement.

(b) This Agreement shall survive assignment, and the assignor and any permitted assignee shall be bound by it.

**14. DURATION AND TERMINATION**

(a) This Agreement is in effect as long as there is an active License for a Product and/or Support.

(b) Customer may terminate this Agreement unilaterally, at any time and without cause, by providing at least three (3) months' prior written notice to SonarSource or in accordance with GSA Schedule Contract Clause 552.212-4(l) or (m).

(c) When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, SonarSource shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Immediately upon receipt of SonarSource's termination notification (which may be oral or in writing), Customer shall:

(i) cease using the Product;
(ii) cease requesting Support;
(iii) destroy any corresponding License Keys; and
(iv) provide SonarSource with written confirmation of such destruction within fifteen (15) days from the termination date.

(d) Reserved.

(e) The following sections shall survive termination of this Agreement: Sections 6 (Personal Information), 7 (Confidentiality), 8 (Customer's Obligations), 10 (Disclaimer), 11 (Limitation of Liability), 12 (Logo Right), 16 (Governing Law and Jurisdiction), and 17 (General Conditions).

**15. FORCE MAJEURE**

In accordance with GSAR Clause 552.212-4(f), Neither Party shall be deemed in default or otherwise be liable under this Agreement (except for payments due) as a result of its inability to perform its obligations hereunder by reason of any fire, earthquake, flood, substantial snow storm, epidemic, accident, explosion, casualty, strike, lock-out, labor controversy, riot, civil disturbance, act of public enemy, embargo, war, act of God, or any municipal, county, state, provincial, territorial or national ordinance or law, or any executive, administrative or judicial order (which order is not the result of any act or omission which would constitute a default hereunder) or any failure or delay of any transportation, power or communication system or any other similar cause beyond that Party's control.

**16. GOVERNING LAW AND JURISDICTION**

(a) This Agreement is deemed to have been made under and shall be governed by and construed in accordance with the Federallaw of the United States.

(b) Reserved.

**17. GENERAL CONDITIONS**

(a) This Agreement constitutes the Parties' entire contractual relationship. It cancels and supersedes all prior oral or written communications, proposals, conditions, representations, and warranties, and prevails over any conflicting or additional terms mentioned in any price quotation, purchase order, acknowledgment, clickwrap or clickthrough provisions, or other communication between the Parties, regardless of when such terms were issued. This Agreement may only be amended or overridden by a written document, signed by authorized representatives of both Parties.

(b) The English version of this Agreement is the only valid version. Translations into other languages are not legally binding.

(c) Any notices to be provided under this Agreement should be sent by international courier service to the registered address of the Party, or to such other address as that Party may request in writing that notices be sent to.

Notices may also be sent by e-mail if proof of receipt is obtained. E-mail notices to SonarSource must be sent to contact@sonarsource.com.

(d) SonarSource will notify Customer of any material modifications to this Agreement at least 30 days prior to the modifications taking effect by posting a notice on the Website or sending an email notice to Customer. Customer's continued use of a Product and/or Support after thirty (30) days from notice constitutes agreement to the non-material modifications of the Agreement. Material modifications must be bilaterally agreed to by both parties in writing.

**SONAR**

**SonarQube Advanced Security Addendum**

Last Updated August 12, 2025

This Addendum governs Customer's installation and use of SonarQube Advanced Security ("**SQAS**") and related Support. This Addendum is incorporated by reference into, and forms an integral part of, the Agreement between SonarSource and Customer. All capitalized terms used herein but not otherwise defined shall have the meanings given to them in the Agreement.

**1. DEFINITIONS**

1.1 "**Addendum**" means this SQAS Addendum.

1.2 "**Agreement**" means the relevant SonarQube Server Terms and Conditions or the SonarQube Cloud Terms of Service, as applicable, between Customer and SonarSource.

1.3 **"Authorized Use"** means Customer's use of a Sonar Offering in compliance with the terms and conditions of the Agreement, including any associated payment requirements.

1.4 "**Dependency Data**" means lockfiles, manifests, and any other metadata regarding third-party software dependencies, made available by Customer for the purpose of analyzing software dependencies and components.

1.5 **"SQAS License**" means a separate, supplementary license granted to Customer to use SQAS solely in conjunction with an approved Sonar Offering. The SQAS License cannot operate independently of the corresponding permissions granted by the Agreement for the associated Sonar Offering.

1.6 "**Security Analysis Results**" means the results that are generated by SQAS processing Dependency Data, and made available to Customer via SQAS.

1.7 **"Sonar Offering"** means the Product (as defined in the SonarQube Server Terms and Conditions) or the Service (as defined in the SonarQube Cloud Terms of Service), as applicable.

**2. INTELLECTUAL PROPERTY**

2.1 Subject to the terms, conditions, and limitations of the Agreement and this Addendum, SonarSource grants Customer a worldwide, non-exclusive, non-transferable, non-sublicensable and revocable SQAS License: (i) for the use of SQAS together with the Authorized Use of the Sonar Offering; and (ii) to access, use, and distribute the Security Analysis Results and Documentation for Customer's own internal software development

purposes. The SQAS License is limited to the usage tier and term set forth in the applicable sales documents.

2.2 As between the Customer and SonarSource, all right, title, and interest in and to Dependency Data, including all Intellectual Property rights therein, belong exclusively to Customer. Customer grants to SonarSource the right to internally use such data for the purpose of providing the Customer with SQAS, Documentation, and Security Analysis Results.

2.3 Except for the limited license rights expressly granted by SonarSource to Customer in Section 2.1 above, all right, title, and interest in and to SQAS, Documentation, and Security Analysis Results, including all Intellectual Property rights therein, belong exclusively to SonarSource and/or its licensors. All rights not expressly granted under this Addendum are reserved by SonarSource. Customer undertakes to comply with and not to challenge or misuse any of SonarSource's Intellectual Property rights.

2.4 SonarSource is hereby granted a royalty-free, fully-paid, worldwide, exclusive, transferable, sub-licensable, irrevocable, and perpetual license to use or incorporate into its products and services any suggestions, enhancement requests, recommendations, or other feedback provided by you relating to SQAS or Documentation.

**3. CUSTOMER'S OBLIGATIONS**

All terms and conditions applicable to the use of the Sonar Offering under the Agreement apply to Customer's use of SQAS.

**4. CUSTOMER AND PERSONAL INFORMATION**

4.1 SQAS transmits Dependency Data to SonarSource's cloud servers for analysis, but does not transmit Customer's source code. SonarSource has implemented physical, administrative, organizational, and technical information security measures to protect the security of Dependency Data.

4.2 By design, Dependency Data does not include Personal Data. However, if Customer includes Personal Data within the Dependency Data, SonarSource disclaims all liability.

4.3 Sonarsource shall implement the appropriate technical and organizational measures to secure the Dependency Data described in Schedule 3 of the Data Processing Addendum available at sonarsource.com/legal/data-processing-addendum/

**5. SUPPORT AND SERVICE LEVEL COMMITMENT**

If Customer purchased Support or is otherwise entitled to receive Support, SonarSource will provide Support for SQAS in accordance with the Agreement. SonarSource will provide

SQAS's network-dependent functionalities in accordance with the applicable Service Level Agreement.

**6. MODIFICATION TO THE SERVICE**

SonarSource may make commercially reasonable updates or modifications to SQAS from time to time to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of system use, and availability of a third-party program. SonarSource will provide advance notice of any such material updates or modifications that it reasonably believes are likely to materially degrade core features or functionalities of SQAS.

**7. GENERAL**

Except as modified by this Addendum, the Agreement remains in full force and effect. SonarSource may non-materially modify this Addendum from time to time. SonarSource will notify Customer of any material modifications to this Addendum at least thirty (30) days prior to such modifications taking effect, either by posting a notice on the Website or by sending an email notice to Customer. Customer's continued use of SQAS and/or Support after thirty (30) days from such notice will constitute Customer's acceptance of the non-material modifications to this Addendum. In the event of any conflict between the terms of this Addendum and the Agreement, the terms of this Addendum shall prevail in connection with SQAS.

**COMMERCIAL SUPPORT**

**Terms and conditions**

Last updated April 1, 2024

Sonar Commercial Support is a private communication channel between you and the Sonar team to provide guidance and solve issues during the implementation and use of active versions of select commercial editions of SonarQube Server and SonarQube Cloud.

The terms of Sonar Commercial Support are subject to non-materially change without notice. Use of Sonar Commercial Support is subject to the attached SonarQube Server Terms & Conditions, , or, if applicable, a negotiated custom agreement, and the Sonar Privacy Policy.

There are two levels of Sonar Commercial Support: Standard Support and Premium Support.

**Sonar Standard Support**

Sonar Standard Support is available for active versions of SonarQube Server Developer, Enterprise, and Data Center Editions, as well as SonarQube Cloud. Our team of qualified support engineers will work to diagnose and solve issues related to cases you file in our support portal. We aim to provide a first response to all issue categories within one business day, and will use commercially reasonable efforts to prioritize Blocker and Critical issues. All Support communication is in English.

**Sonar Premium Support**

Sonar Premium Support is available for active versions of SonarQube Server Developer, Enterprise, and Data Center Editions. Premium Support guarantees Service Level Agreement response times based on issue criticality, with dedicated senior support engineers ready to help ensure your business continues to operate with minimal disruption. All support communication is in English, and Sonar will send a quarterly report summarizing all issues and SLAs via email.

**Service Level Agreement response times**

For premium support cases you file in our support portal, the initial response time guaranteed by the SLA is dependent on the criticality of the ticket (see the issue severity categories in the section below). An initial response does not mean the issue has been resolved. **Blocker** issues will have 24-hour/7-day support with a 1-hour initial response SLA. **Critical** issues will have 24-hour/5-day support with a 4-hour initial response SLA. **Major** and **Minor** issues will have a 1-business day initial response SLA. If a Blocker

issue requires immediate attention on a weekend, you must call the provided support phone number.

**Receiving credits for missed responses to premium support tickets**

If you do not receive an initial response within the guaranteed response time to more than four tickets in a given quarter (based on Sonar's fiscal year), you may be eligible for a credit. To honor the SLA, Sonar will credit your account in an amount equal to 25% of your annual Sonar Premium Support fee. To receive the credit, you must submit a credit request.

The credit request must be made within 30 days of the end of the quarter during which Sonar Premium Support did not respond to your tickets within the designated response time. Credit requests will not be honored if the respective deadline has passed. Credits cannot be exchanged into a cash amount, require you to have paid any outstanding invoices, and expire upon termination of your agreement with Sonar.

To receive a credit, you must submit a completed credit request to supportcredits@sonarsource.com. To be eligible, the credit request must:

- Be sent from an email address associated with your account on SonarSource.com;
- Be received by SonarSource by the end of the 30th day after the quarter in which the qualifying tickets occurred;
- Include "Credit Request" in the subject line.

The following information must be included in your credit request:

- **Date**: The date must be within 30 days after the quarter based on Sonar's fiscal year end in which the tickets occurred (March 31, June 30, September 30, December 31);
- **Customer Contact**: Specify your name and email address;
- **Customer Address**: Specify your company address;
- **Qualifying Tickets**: Provide the date of each qualifying ticket;
- **Ticket Numbers**: Provide the ticket number of each qualifying ticket.

**Categories of issue severity**

Our Support team will categorize your ticket based on the following issue severity guidelines. Sonar has the sole discretion to modify the category of a ticket at any time and may lower the category after determining and mitigating the primary cause of an issue.

| Severity | Impact | Examples |
| --- | --- | --- |
| **Blocker** | Production outages with a major impact on business-critical operations | • SonarQube instance is down, unavailable, or unresponsive;<br>• All users in the organization are unable to login;<br>• All analysis is failing or background tasks are not processing;<br>• Production upgrade is halted or unresponsive. |
| **Critical** | A material degradation in responsiveness with important features or capabilities unavailable or extremely slow.A material degradation in responsiveness with important features or capabilities unavailable or extremely slow. | • Sudden shutdown; restart worked but the system seems unstable;<br>• UI works fine but many analyses are failing or background tasks are piling up (but still processing);<br>• UI cannot be browsed efficiently; web navigation seems to suffer many errors and/or performance issues<br>• Blocker scenario, but in a staging environment. |

| | | |
|---|---|---|
| **Major** | Issues impact a limited subset of functionalities or users or a non-business critical environment. | • A single user is unable to login;<br>• An analysis is failing on one or more projects, but not all;<br>• Unstable system with tool crashes that don't resolve after restart;<br>• License/subscription that is about to expire beyond the 14-day grace period;<br>• A secondary SonarQube environment is down or non-functional. |
| **Minor** | Product questions or enhancement requests. | • Basic functional questions;<br>• Suggestions for a capability request, change, or improvement;<br>• Issues that may appear as real issues but are in fact known limitations. |

**SONAR**

**Data processing addendum**

Last updated November 3, 2025.

*Notice: Please note that we have updated our Data Processing Addendum. Existing customers may continue under the prior version until December 2, 2025*

This Data Processing Addendum ("**DPA**") supplements the SonarQube Server Terms and Conditions, the SonarQube Cloud Terms of Service or other agreement in place between Customer and SonarSource (the "**Agreement**") covering Customer's use of SonarQube Server, SonarQube Cloud, Sonar Support, or any other SonarSource products or services to which this DPA applies (the "**Products**"). Capitalized terms not defined in this DPA have the meanings set forth in the relevant Agreement.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. **Definitions.**

- "**Affiliate**" means an entity that, directly or indirectly, owns or controls, is owned or is controlled by or is under common ownership or control with a party, where "ownership" means the beneficial ownership of more than fifty percent (50%) of an entity's voting equity securities or other equivalent voting interests and "control" means the power to direct the management or affairs of an entity.
- "**Applicable Data Protection Law**" means all data protection laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, and may include the additional definitions provided for in Schedule 2 herein.
- "**Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- "**Customer**" means the customer entity or individual that is the contracting party to the Agreement.
- "**Customer Data**" means (i) any data, including source code, configuration files, or related materials, that Customer inputs into or transmits through the Products in

connection with its use of the Products, and (ii) any related materials, such as code snippets, configuration files, screenshots, or logs that Customer or its Users provide to SonarSource in connection with Support requests.

- "**Customer Personal Data**" means any Personal Data contained in Customer Data that SonarSource Processes under the Agreement solely on behalf of Customer.
- "**Personal Data**" means any information that relates to an identified or identifiable natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Applicable Data Protection Law.
- "**Processing**" (and "**Process**") means any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- "**Processor**" means the entity that Processes Personal Data on behalf of the Controller.
- "**Security Incident**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by SonarSource and/or its Sub-processors.
- "**Sub-processor**" means any third party engaged by SonarSource in its role as a Processor to Customer to Process Customer Personal Data.
- "**Term**" means the term of this DPA which begins with the commencement of the term of the Agreement and terminates upon expiration or earlier termination of the Agreement (or, if later, the date on which SonarSource ceases all Processing of Customer Personal Data).
- "**User**" means any individual that Customer authorizes to use the Products. Users may include: (i) Customer's and its Affiliates' employees, consultants, contractors and agents, (ii) third parties with which Customer or its Affiliates transact business, (iii) individuals invited by Customer's users, (iv) individuals under managed accounts, or (v) individuals interacting with a Product as Customer's customer.

2. **Scope**.

2.1 *Customer Personal Data*. SonarSource will Process Customer Personal Data as Customer's Processor in accordance with Customer's instructions as outlined in Section 3.1 (Customer Instructions). Customer agrees that any Customer Personal Data it submits as part of its use of the Products will be done in accordance with the requirements of Applicable Data Protection Law and the Agreement, and Customer will, if applicable, provide notice to, and obtain the necessary rights and consents from, data subjects concerning the Customer's use of the Product. Customer shall have sole responsibility for the accuracy, quality and legality of Customer Personal Data and the means by which Customer or any relevant third-party acquired Customer Personal Data.

2.2 *Description of the Processing*. Details regarding the Processing of Customer Personal Data by SonarSource are stated in Schedule 1 (Description of Processing).

2.3 *International Applicability*. To the extent SonarSource Processes Customer Personal Data protected by Applicable Data Protection Law in one of the regions listed in Schedule 2 (Region-Specific Terms), the terms specified for the applicable regions will also apply, including the provisions relevant for international transfers of Customer Personal Data (directly or via onward transfer).

2.4 *Order of Precedence*. If there is any conflict or inconsistency among the following documents, the order of precedence is: (1) the applicable terms stated in Schedule 2 (Region-Specific Terms including any transfer provisions); (2) the main body of this DPA; and (3) the Agreement.

2.5 *Updates*. SonarSource may modify this DPA as required due to (a) changes in Applicable Data Protection Law; or (b) the release of new features, functions, products or services or material changes to any of the existing Products. SonarSource may make such modifications by posting a revised version of this DPA at sonarsource.com, or by otherwise sending an email to the primary email address specified in Customer's Account.

2.6 *Cumulative claims*. Any claims against SonarSource or its Affiliates under this DPA can only be brought against SonarSource by the Customer entity that is a party to the Agreement.

2.7 *Liability*. The total aggregate liability of SonarSource and its Affiliates arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, will be subject to the same limitations and exclusions of liability as apply under the Agreement, whether any such liability arises under the Agreement or this DPA.

2.8 *Governing law and jurisdiction*. This DPA will be governed by and construed in

accordance with the governing law and jurisdiction provisions in the Agreement unless required otherwise by Applicable Data Protection Law.

2.9 *Entire agreement*. This DPA supersedes any prior agreements between Customer and SonarSource concerning the privacy, data protection, and security requirements that apply to the processing of Customer Personal Data. Except where expressly approved by SonarSource in writing, any deletions or revisions to this DPA by Customer shall be null and void.

3. **Processing**.

3.1 *Customer Instructions*. SonarSource will Process Customer Personal Data in accordance with the documented lawful instructions of Customer as stated in the Agreement (including this DPA), the applicable SonarSource order forms, Customer's use of the Products (including relevant configuration and settings), and the provision of related Support, as necessary to (i) enable the use of various features and functionalities of the Products in accordance with the Documentation, (ii) provide, operate, maintain, enhance, and improve the products and services provided by SonarSource, (iii) act as directed by Users through the Products, including investigating Security Incidents and resolving issues, bugs, and errors, or (iv) comply with its legal obligations. SonarSource will notify Customer if it becomes aware, or reasonably believes, that Customer's instructions violate Applicable Data Protection Law.

3.2 *Confidentiality*. SonarSource will treat Customer Personal Data as Customer's Confidential Information under the Agreement. SonarSource will ensure personnel authorized to Process Customer Personal Data are bound by written or statutory obligations of confidentiality.

4. **Security**.

4.1 *Security Measures*. SonarSource implements and maintains appropriate technical and organizational measures designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents. Customer is responsible for configuring the Products and using features and functionalities made available by SonarSource to maintain appropriate security in light of the nature of Customer Personal Data. Schedule 3 (Technical and Organizational Measures) describes SonarSource's current technical and organizational measures. Customer acknowledges that the security measures are subject to technical progress and development and that SonarSource may update or modify the security measures from time to time, provided that

such updates and modifications do not materially decrease the overall security of the Products during the Term.

4.2 *Security Incidents*. SonarSource will notify Customer without undue delay and, where feasible, no later than seventy-two (72) hours after becoming aware of a Security Incident. SonarSource will make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within SonarSource's reasonable control. Upon Customer's request and taking into account the nature of the Processing and the information available to SonarSource, SonarSource will assist Customer by providing information reasonably necessary for Customer to meet its Security Incident notification obligations under Applicable Data Protection Law. SonarSource's notification of a Security Incident is not an acknowledgment by SonarSource of its fault or liability.

5. **Sub-processing**.

5.1 *Authorization*. Customer provides general authorization for SonarSource to engage Sub-processors to Process Customer Personal Data. SonarSource will: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Customer Personal Data to the standard required by Applicable Data Protection Law and to the same standard provided by this DPA; and (ii) remain liable to Customer for the acts and omissions of its Sub-processor to the same extent SonarSource would be liable if performing the task or service directly under this DPA. SonarSource maintains an up-to-date list of its Sub-processors in its Trust Center.

5.2 *New Sub-processors*. Periodically, SonarSource may engage new Sub-processors. SonarSource will give Customer at least fourteen (14) calendar days' notice prior to providing that Sub-processor with access to Customer Personal Data by updating the Trust Center accordingly ("**Sub-processor Notice Period**"). The Trust Center provides the option for Customer to subscribe to notifications of any new Sub-processors.

5.3 *Objections*. Customer may object to SonarSource's appointment of a new Sub-processor during the Sub-processor Notice Period. If Customer objects, Customer, as its sole and exclusive remedy, may terminate the applicable SonarSource order form for the affected Product in accordance with the terms of the relevant Agreement.

6. **Assistance and Cooperation Obligations**.

6.1 *Data Subject Rights*. Taking into account the nature of the Processing, SonarSource will provide reasonable and timely assistance to Customer to enable Customer to respond to requests for exercising a data subject's rights (including rights of access, rectification, erasure, restriction, objection, and data portability) in respect to Customer Personal Data

(each a "**Data Subject Request**"). Accordingly, SonarSource will refrain from responding to the data subject except to acknowledge receipt of the Data Subject Request and will redirect the data subject to make its request or objection directly to the Customer. SonarSource reserves the right to charge a mutually agreed fee for assistance rendered upon Customer's assistance demands.

6.2 *Cooperation Obligations*. Upon Customer's reasonable request, and taking into account the nature of the applicable Processing, SonarSource will provide reasonable assistance to Customer in fulfilling Customer's obligations under Applicable Data Protection Law (including data protection impact assessments and consultations with supervisory authorities), provided that Customer cannot reasonably fulfill such obligations independently with help of available Documentation. Requests under this Section 6.2 should be made to contact@sonarsource.com or such other location as SonarSource may periodically make available on its Website. SonarSource reserves the right to charge a mutually agreed fee for assistance rendered upon Customer's assistance demands.

6.3 *Third Party Requests*. Unless prohibited by law, SonarSource will promptly notify Customer of any valid, enforceable subpoena, warrant, or court order from law enforcement or public authorities compelling SonarSource to disclose Customer Personal Data. In the event that SonarSource receives an inquiry or a request for information from any other third party (such as a regulator or data subject) concerning the Processing of Customer Personal Data, SonarSource will redirect such inquiries to Customer, and will not provide any information unless required to do so under applicable law.

7. ***Deletion of Customer Personal Data***. During the term of the Agreement, Customer and its Users may, through the features of the Products, access, retrieve or delete Customer Personal Data. Following expiration or termination of the Agreement, SonarSource will delete all Customer Personal Data. Notwithstanding the foregoing, SonarSource may retain Customer Personal Data (i) as required by Applicable Data Protection Law, or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, SonarSource will maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to retained Customer Personal Data and not further Process it except as required by Applicable Data Protection Law.

8. **Audit**.

8.1 SonarSource will be regularly audited against the ISO 27001 standard (or equivalent). The audit may, in SonarSource's sole discretion, be an internal audit, or an audit performed by a third party. Upon written request, SonarSource will provide Customer with a summary of its most recent independent certification or attestation report(s) once every twelve (12)

months during the term of the Agreement ("Audit Information"), so that Customer can verify SonarSource's compliance with the audit standards and this DPA. Such Audit Information constitutes SonarSource's Confidential Information and Customer shall comply with its confidentiality obligations provided for in the Agreement with respect to any Audit Information.

8.2 Only to the extent Customer cannot reasonably satisfy SonarSource's compliance with this DPA through the exercise of its rights under Section 8.1 above, or where required by Applicable Data Protection Law or a supervisory authority, an independent and qualified third party auditor appointed by Customer and approved by SonarSource, may, at Customer's sole expense, audit, during the term of the relevant Agreement, the relevant applicable Personal Data processing activities to assess SonarSource's compliance with the terms of this DPA. Any such audit may occur no more than once per year. Any audit will (i) be conducted during SonarSource's regular business hours, with reasonable advance written notice of at least sixty (60) calendar days (unless Applicable Data Protection Law or a supervisory authority requires a shorter notice period); (ii) be subject to reasonable confidentiality controls obligating Customer (and its authorized representatives) to keep confidential any information disclosed that, by its nature, should be confidential; and (iii) restrict its findings to only information relevant to Customer.

**Schedule 1**

Description of Processing

1. **Categories of data subjects whose Personal Data is Processed**: Customer and its Users.
2. **Categories of Personal Data Processed**: Customer Personal Data.
3. **Sensitive data transferred**: Customer shall ensure that it does not provide any data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) genetic data, biometric data Processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, or (iii) relating to criminal convictions and offenses (altogether "**Sensitive Data**").
4. **The frequency of the transfer**: Continuous.
5. **Nature of the Processing**: SonarSource will Process Customer Personal Data in order to provide the Products and related Support in accordance with the Agreement, including this DPA.

6. **Purpose(s) of the Processing**:
   6.1 SonarSource will Process Customer Personal Data as Processor in accordance with Customer's instructions as set out in Section 3.1 (Customer Instructions)

7. **Duration of Processing**:
   7.1 SonarSource will Process Customer Personal Data for the term of the Agreement as outlined in Section 7 (Deletion of Customer Personal Data).

8. **Transfers to (Sub-)processors:** SonarSource will transfer Customer Personal Data to Sub-processors as permitted in Section 5 (Sub- processing).

**Schedule 2**

Region-Specific Terms

1. **Europe, United Kingdom, and Switzerland**.

1. 1. *Customer Instructions*. In addition to Section 3.1 (Customer Instructions) of the DPA above, SonarSource will Process Customer Personal Data only on documented instructions from Customer, including with regard to transfers of such Customer Personal Data to a third country or an international organization, unless required to do so by Applicable Data Protection Law to which SonarSource is subject; in such a case, SonarSource will inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. SonarSource will promptly inform Customer if it becomes aware that Customer's Processing instructions infringe Applicable Data Protection Law.

1.2 *European Transfers*. Where Customer Personal Data protected by the EU Data Protection Law is transferred, either directly or via onward transfer, to a country outside of Europe that is not subject to an adequacy decision, the following applies:

- (a) The EU SCCs are hereby incorporated into this DPA by reference as follows:
    - (i) Customer is the "data exporter" and SonarSource is the "data importer".
    - (ii) Module Two (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and SonarSource is Processing Customer Personal Data as a Processor.
    - (iii) Module Three (Processor to Processor) applies where Customer is a Processor of Customer Personal Data and SonarSource is Processing Customer Personal Data as another Processor.

- (iv) By entering into this DPA, each party is deemed to have signed the EU SCCs as of the commencement date of the Agreement.

- (b) For each Module, where applicable:
  - (i) In Clause 7, the optional docking clause does not apply.
  - (ii) In Clause 9, Option 2 applies, and the time period for prior notice of Sub-processor changes is stated in Section 5 (Sub- processing) of this DPA.
  - (iii) In Clause 11, the optional language does not apply.
  - (iv) In Clause 17, Option 1 applies, and the EU SCCs are governed by Irish law.
  - (v) In Clause 18(b), disputes will be resolved before the courts of Ireland.
  - (vi) The Appendix of EU SCCs is populated as follows:
    - The information required for Annex I(A) is located in the Agreement and/or relevant SonarSource order forms.
    - The information required for Annex I(B) is located in Schedule 1 (Description of Processing) of this DPA.
    - The competent supervisory authority in Annex I(C) will be determined in accordance with Clauses 17, Option 1 and 18(b) above; and
    - The information required for Annex II is located in Schedule 3 (Technical and Organizational Measures).

1.3 *Swiss Transfers*. Where Customer Personal Data protected by the Swiss FADP is transferred, either directly or via onward transfer, to any other country that is not subject to an adequacy decision, the EU SCCs apply as stated in Section 1.2 (European Transfers) above with the following modifications:

- (a) All references in the EU SCCs to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss FADP, and references to specific Articles of "Regulation (EU) 2016/679" will be replaced with the equivalent article or section of the Swiss FADP; all references to the EU Data Protection Law in this DPA will be interpreted as references to the Swiss FADP.
- (b) In Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

- (c) In Clause 17, the EU SCCs are governed by the laws of Switzerland.
- (d) In Clause 18(b), disputes will be resolved before the courts of Switzerland.
- (e) All references to Member State will be interpreted to include Switzerland and data subjects in Switzerland are not excluded from enforcing their rights in their place of habitual residence in accordance with Clause 18(c).

1.4 *United Kingdom Transfers*. Where Customer Personal Data protected by the UK Data Protection Law is transferred, either directly or via onward transfer, to a country outside of the United Kingdom that is not subject to an adequacy decision, the following applies:

- (a) The EU SCCs apply as set forth in Section 1.2 (European Transfers) above with the following modifications:
    - (i) Each party shall be deemed to have signed the UK Addendum.
    - (ii) For Table 1 of the UK Addendum, the parties' key contact information is located in the Agreement and/or relevant SonarSource order forms.
    - (iii) For Table 2 of the UK Addendum, the relevant information about the version of the EU SCCs, modules, and selected clauses which this UK Addendum is appended to is located above in Section 1.2 (European Transfers) of this Schedule.
    - (iv) For Table 3 of the UK Addendum:
        - The information required for Annex 1A is located in the Agreement and/or relevant SonarSource order forms.
        - The Information required for Annex 1B is located in Schedule 1 (Description of Processing) of this DPA.
        - The information required for Annex II is located in Schedule 3 (Technical and Organizational Measures); and
        - The information required for Annex III is located in Section 5 (Sub-processing) of this DPA.
    - (v) In Table 4 of the UK Addendum, "neither party" was selected.

**2. United States of America**. The following terms apply where SonarSource Processes Customer Personal Data subject to the US State Privacy Laws:

2.1 To the extent Customer Personal Data includes personal information protected under US State Privacy Laws that SonarSource Processes as a Service Provider or Processor, on

behalf of Customer, SonarSource will Process such Customer Personal Data in accordance with the US State Privacy Laws, including by complying with applicable sections of the US State Privacy Laws and providing the same level of privacy protection as required by US State Privacy Laws, and in accordance with Customer's written instructions, as necessary for the limited and specified purposes identified in Section 2.1 (Customer Personal Data) and Schedule 1 (Description of Processing) of this DPA, which are deemed "business purposes" under US State Privacy Laws. SonarSource will not:

- (a) retain, use, disclose or otherwise Process such Customer Personal Data for a commercial purpose other than for the limited and specified purposes identified in this DPA, the Agreement, and/or any related SonarSource order form, or as otherwise permitted under US State Privacy Laws;
- (b) "sell" or "share" such Customer Personal Data within the meaning of the US State Privacy Laws; and
- (c) retain, use, disclose or otherwise Process such Customer Personal Data outside the direct business relationship with Customer and not combine such Customer Personal Data with personal information that it receives from other sources, except as permitted under US State Privacy Laws.

2.2 SonarSource will inform Customer if it determines that it can no longer meet its obligations under US State Privacy Laws within the timeframe specified by such laws, in which case Customer may take reasonable and appropriate steps to prevent, stop, or remediate any unauthorized Processing of such Customer Personal Data.

2.3 To the extent Customer discloses or otherwise makes available Deidentified Data to SonarSource or to the extent SonarSource creates Deidentified Data from Customer Personal Data, in each case in its capacity as a Service Provider, SonarSource will:

- (a) adopt reasonable measures to prevent such Deidentified Data from being used to infer information about, or otherwise being linked to, a particular natural person or household;
- (b) publicly commit to maintain and use such Deidentified Data in a de-identified form and to not attempt to re-identify the Deidentified Data, except that SonarSource may attempt to re-identify such data solely for the purpose of determining whether its de-identification processes are compliant with the US State Privacy Laws; and
- (c) before sharing Deidentified Data with any other party, including Sub-processors, contractors, or any other persons ("**Recipients**"), contractually obligate any such

Recipients to comply with all requirements of this Section 2.3 (including imposing this requirement on any further Recipients).

3. Definitions.

3.1 Where Customer Personal Data is subject to the laws of one the following regions, the definition of "**Applicable Data Protection Law**" includes:

- (a) **Europe**: (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation, or GDPR) and (ii) the EU e-Privacy Directive (Directive 2002/58/EC) as amended, superseded or replaced from time to time ("**EU Data Protection Law**");
- (b) **Singapore**: the Singapore Personal Data Protection Act;
- (c) **Switzerland**: the Swiss Federal Act on Data Protection and its implementing regulations as amended, superseded, or replaced from time to time ("**Swiss FADP**");
- (d) **The United Kingdom**: the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 as amended, superseded or replaced from time to time ("**UK Data Protection Law**"); and
- (e) **The United States**: all state laws relating to the protection and Processing of Personal Data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations ("**CCPA**"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act ("**US State Privacy Laws**").

3.2. "**Deidentified Data**" means data that cannot reasonably be used to infer information about, or otherwise be linked to, a data subject.

3.3. "**Europe**" includes, for the purposes of this DPA, the Member States of the European Union and European Economic Area.

3.4. "**EU SCCs**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, superseded, or replaced from time to time.

3.5. "**Service Provider**" has the same meaning as given in the CCPA.

3.6. "**UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022, as amended, superseded or replaced from time to time.

**Schedule 3**

Technical and Organizational Measures including Technical and Organizational Measures to ensure the security of the data

Access Control

- Internally, SonarSource restricts access to Customer Personal Data to its employees or contractors who have a defined need-to-know basis or a role requiring such access.
- Internally, access to the SonarSource network and production systems requires multi-factor authentication (MFA), or equivalent controls.
- Internally, SonarSource maintains user access controls that address the timely provisioning and de-provisioning of SonarSource employee and contractor internal user accounts.
- Remote access is strictly managed and requires secure connections and MFA to access the SonarSource network and production environments.

Personnel Security

- SonarSource performs appropriate educational and criminal background checks on its employees and contingent workers, as applicable under the relevant local laws and regulations.
- SonarSource ensures that all of SonarSource's employees and contingent workers receive security awareness and data protection training appropriate for their role upon hire, as well as update training sessions at least annually thereafter.

Audit

- Internally, and for the Products, SonarSource will maintain ISO 27001:2022 certification and/or AICPA SOC 2 attestation for the term of the Agreement.
- SonarSource agrees to participate in Customer's third-party assurance program. SonarSource agrees to complete Customer's security questionnaires at intervals of

every twelve (12) months, or upon contract renewal(s), where the information provided in SonarSource's security certification or attestation reports is deemed insufficient to answer to assurance questions.

Business Continuity

- SonarSource maintains business continuity, backup and disaster recovery plans ("**BC/DR Plans**") in order to minimize the loss of service and to comply with Applicable Data Protection Law.
- The BC/DR Plans address threats to the Products and any dependencies, and have an established procedure for resuming access to, and use of, the Products.
- SonarSource tests the BC/DR Plans at regular intervals.
- SonarSource enables all Customer Product instances with a minimum of thirty (30) days' of back-ups, to which only the Customer has access to.
- All customer instances enabled within the AWS Frankfurt region use High Availability (HA) configuration.
- For Customer's own environments and systems, the Customer is solely responsible for the design, development, implementation, and management of its own BC/DR Plans, including the use of the supplied back-ups provided by SonarSource.

Change Control

- SonarSource maintains internal policies and procedures for applying changes to the Products, including the underlying infrastructure and system components, to ensure quality standards are being met.
- SonarSource undergoes a penetration test of its network, Products and Support offerings on an annual basis. Any vulnerabilities found during this testing are remediated in accordance with SonarSource's Vulnerability Management Policies and Procedures and are assessed on the basis of Sonar's Risk Management Framework.
- SonarSource performs regular scans of its network and any vulnerabilities found will be addressed in accordance with SonarSource's Vulnerability Management Policies and Procedures and are assessed on the basis of Sonar's Risk Management Framework.
- Security patches are applied in accordance with SonarSource's patching schedule.

Data Classification and Security

- SonarSource maintains and enforces formal data classification and handling requirements for all customer, internal, and public-facing data.
- SonarSource maintains technical safeguards and other security measures to ensure the security and confidentiality of Customer Personal Data, including state of endpoint device protections, anti-malware, IDS/IPS, data loss/leakage prevention (DLP), network and host-based firewalls.
- Sonar logically segregates Customer Personal Data in the production environment.

Logging and Monitoring

- SonarSource logs and correlates all material events from its internal and production environments through SIEM technology, with 24x7x365 security alert and monitoring from its Service Operations Center.
- SonarSource logically segregates all Customer instance and production logs and events.

Vulnerability Management

- SonarSource regularly scans internal and production environments for vulnerability and remediates in a timely manner.

**Sonar**

**Privacy Notice**

*Last updated November 3rd, 2025*

At SonarSource, we are committed to protecting your personal data and being transparent about how we handle it. This Privacy Notice ("Notice") explains what personal data we collect, how we use it, and your choices regarding your information. In this Notice, "personal data" and "personal information" refer to information that can identify you directly or indirectly, but do not include anonymous or aggregated data.

This Notice applies to personal data collected by SonarSource Sàrl and our affiliates ("SonarSource", "we", "us", or "our") when you interact with our websites ("Sites"), use our products and services ("Services"), or engage with us through channels such as customer support, events, marketing, or product research. It applies only to personal data for which SonarSource is the  data controller.

Please note, this Notice does not cover how third-party applications, software, or services that may integrate with ours, or any other third-party offerings governed by their own privacy policies, will use your personal data.

We encourage you to read this Notice carefully. If you have questions or concerns, please contact us using the details provided at the end of this Notice.

**Account Users under Organizations**

If you access our Sites or Services as part or on behalf of an organization (such as your employer, company, or another entity), your use may be subject to that organization's policies and administrative controls. In these cases, your organization may manage your account, set usage permissions, and access or process your personal data in connection with your use of our Sites and Services.

SonarSource collects and processes personal data about account users under organizations as described in the "What Information We Collect" section of this Notice. In addition, we may disclose relevant personal data to authorized representatives of your organization to facilitate account administration, support requests, and compliance with organizational policies.

Your organization is responsible for ensuring that any personal data it provides to SonarSource, or requests us to process, complies with applicable data protection laws. For questions about how your organization handles your personal data, please contact your organization's administrator or refer to their privacy policy.

**What Information We Collect**

We collect personal data in several ways, including directly from you, automatically from your devices, and from third parties.

**1. Information You Provide to Us**

We collect personal data when you:

- Sign up or create an account on our Sites or Services.
- Use our Services.
- Contact support.
- Participate in events, product research, or user experience activities.
- Sign up for marketing communications, newsletters, or events via web forms or other marketing activities.
- Communicate with us or provide feedback.

This may include:

- **Account and Profile Information:** Name, email address, mailing address, phone number, user ID, employer name and registered address, job title, and other identifiers assigned by your employer or organization.
- **Payment Information:** Payment and billing details, transaction history.
- **Product Analysis Data**: Information generated by our Services from processing customer-provided content (such as source code or project metadata). While our Services do not require personal data in scanned content, if included as part of the content you choose to scan, we may incidentally process details such as names of software developers found in code comments, commit messages, project descriptions, or integration metadata.
- **Support Data:** Details relevant to support requests, such as descriptions, code samples, screenshots, logs, or other files.
- **Feedback and Survey Data:** Responses to surveys, reviews, feedback forms, and interactive features, including written, audio, or video submissions. Where required by law, we will obtain your explicit consent before collecting audio or video recordings. You may withdraw your consent at any time by contacting us using the details provided at the end of this Notice.

- **Sales and Marketing Data:** Information for promotional communications, such as name, email, employer name and registered address, job title, and marketing preferences. You may opt out of receiving promotional emails or withdraw your consent at any time; instructions for opting out and withdrawing your consent are provided at the end of this Notice.
- **Sales Call Recordings and Transcriptions**: Our Sales Team may record calls for training, quality assurance, service improvement, and to facilitate business transactions. Where required by law, we will obtain your explicit consent before recording any calls. You may withdraw your consent at any time by contacting us using the details provided at the end of this Notice. We may use AI-powered tools to transcribe and analyze these recordings to enhance our sales processes and customer experience. These transcriptions are treated as personal data and handled in accordance with this Notice.

**2. Information Collected Automatically**

When you access our Sites or Services, we automatically collect data from your devices using cookies, web beacons, device identifiers, pixels, and similar technologies to operate, secure, and improve our Sites and Services. The information we collect using these tools includes:

- **Technical and Usage Data:** Device type, browser, operating system, log files, error reports, system configuration, access times, browsing activity, session details, referring site, pages viewed, and links clicked.
- **Location Data:** General location inferred from IP address, device settings, or other information.
- **Website Usage Data:** Interactions with our Sites, such as pages visited, features used, time spent, navigation paths, search queries, clickstream data, and content interactions. Some of this data may be collected through cookies or similar technologies as described above.
- **Inferences and Preferences:** We may derive insights about your interests, preferences, or characteristics based on your activity, purchase history, or interactions with our Sites and Services.

For more details and opt-out options with respect to our use of cookies and similar technologies, see our Cookie Policy.

**3. Information from Third Parties**

We may receive personal data about you from:

- Business and channel partners, resellers, marketing and lead generation providers, public sources, our affiliates, or other users.
- Third-party applications or services you choose to integrate or link with our Services. When you connect your account to a third-party application, you authorize SonarSource to receive information from that application as permitted by your settings and the third party's privacy policies.

This may include:

- **Account and Profile Information:** Name, email, employer, job title, or other contact details.
- **Sales and Marketing Data:** Information for promotional, sales, or marketing purposes.
- **Integration Data:** Information received from authentication providers or third party services that you choose to link or integrate with our Services**.**
- **Additional Information:** Data from public sources or other third parties relevant to your interactions with SonarSource.

**How We Use Your Information**

We use the personal data we collect for the following purposes, depending on how you access our Sites, use our Services, and interact with SonarSource:

- **To provide, maintain, and improve our Sites and Services**: Deliver, operate, and support our offerings, including account management, processing transactions, accounting, billing, meeting tax obligations, resolving technical issues, and ensuring reliability, security, and accessibility.
- **To communicate with you**: Respond to inquiries, send administrative information, and provide updates, including via email, about our Sites, Services, events, or policy changes.
- **To personalize your experience**: Tailor content, recommendations, and communications based on your preferences and usage.
- **To record and transcribe sales calls**: with your consent, where required, use recordings and transcriptions for training, quality assurance, service improvement, and business transactions. We may use AI tools for transcription and analysis. You may withdraw your consent at any time.

- **To improve our Services and develop new features**: Analyze usage data and feedback, monitor performance, conduct research and testing, enhance security, update features, and develop new products and services to better meet user need.
- **For events, research, and user experience activities**: Register and manage your participation in events, surveys, interviews, early access testing, and feedback sessions.
- **For marketing and promotional purposes**: With your consent where required, send marketing communications, promotional offers, and information about our Services and events. You may opt out or withdraw your consent at any time; see the end of this Notice for details.
- **To ensure security and prevent misuse**: Monitor, detect, and prevent fraudulent activity, unauthorized access, policy violations, and other harmful or illegal activities.
- **To comply with legal obligations**: Process personal data as required by applicable laws, regulations, or governmental requests.
- **To protect and enforce our legitimate interests and legal rights**: Support audits, legal claims, investigations, and corporate transactions such as mergers or asset transfers.

**How We Disclose Your Personal Data**

We may disclose your personal data to third parties as needed to operate our business, provide our Sites and Services, and comply with legal obligations:

- **Affiliates**: We disclose personal data to SonarSource affiliates to deliver and support our Sites and Services and for internal business operations.
- **Service Providers and Partners**: We engage trusted third-party service providers (processors or subprocessors) to assist with hosting, analytics, payment processing, support, marketing, security, sales call recording and transcription and other business operations. These providers may access personal data only as necessary to perform their services for us, and are contractually required to protect your information. We may also disclose personal data to business partners, resellers, and distributors who help deliver, sell, or implement our Services. If you interact directly with these partners, their privacy policies will apply.

- **Third-Party Authentication and Integrations**: We may enable you to use third-party services to log in to our Services, such as using your GitHub, Bitbucket, GitLab, or Azure DevOps credentials.
- **Legal Requirements and Protection**: We may disclose personal data to comply with laws, regulations, or legal requests, or to enforce our agreements, protect rights and safety, prevent fraud, or address security and technical issues. We may also disclose data to manage legal claims or disputes.
- **Customers and Account Administrators**: As further set out in the "Account Users and Organizations" section.
- **Other Users and Public Forums**: Information you submit in public forums, such as the Sonar Community, may be visible to other users or the public.

**Cookies and Similar Technologies**

SonarSource uses cookies and similar technologies—including pixels, tags, web beacons, JavaScript, and device identifiers—to enhance your experience, analyze usage, and support the functionality of our Sites and Services. Together with our third-party partners, such as analytics providers, we use these technologies to deliver site functionality, recognize you across devices, provide personalized content, analyze performance, and support customization and marketing.

You can manage your cookie preferences and opt out of certain analytics tools at any time. In addition, SonarSource recognizes and honors browser-based opt-out signals, such as the Global Privacy Control ("GPC"), where required by law. If your browser or extension sends a GPC signal, we will treat it as a valid request to opt out of the sale or sharing of your personal information, in accordance with applicable laws in your jurisdiction.

For more information about the cookies we use, your choices, and browser-based opt-out signals such as GPC, please see our Cookie Policy or visit https://globalprivacycontrol.org.

**Data Retention**

We retain personal data only as long as necessary to fulfill the purposes for which it was collected, including providing our Sites and Services, managing your account, and meeting legal or business obligations. Data may be kept longer than is typical to resolve disputes, enforce agreements, or protect legal interests.

Retention periods depend on the type of data, our relationship with you, and applicable legal requirements. When no longer needed, personal data is securely deleted, anonymized, or disposed of in accordance with our policies.

**Data Security**

We protect your personal data using industry-standard technologies and practices, including encryption, access controls, regular security assessments, and employee training. These measures are designed to prevent unauthorized access, disclosure, alteration, or destruction of data and are regularly reviewed and updated.

While we strive to maintain strong security, no method of transmission or storage is completely secure, and no IT infrastructure is immune to unauthorized third-party access or theft. We cannot guarantee the absolute security of your personal data and are not liable for unauthorized third-party actions beyond our reasonable control. Internet transmissions are inherently insecure and are carried out at your own risk; our responsibility applies only once your data is under our control.

We encourage you to protect your account credentials and devices. If you suspect your account or data has been compromised, please contact us promptly using the details at the end of this Notice. For more information about our security practices, please visit our Trust Center.

**Legal Bases for Processing (EEA, UK, and Switzerland)**

If you are located in the EEA, UK, or Switzerland, we process your personal data in line with applicable data protection laws, including the General Data Protection Regulation, UK Data Protection Act, and Swiss Federal Act on Data Protection.

We rely on the following legal bases:

- **Contractual Necessity**: To enter into or perform a contract with you, such as providing our Services or support. Without this data, we may not be able to fulfill our obligations.
- **Legitimate Interests**: To operate, maintain, and improve our Sites and Services, communicate with you, conduct analytics, ensure security, prevent fraud, promote our offerings, and manage legal claims or disputes. We balance these interests against your privacy rights.
- **Legal Obligations**: To comply with laws and regulations, respond to lawful requests, and fulfill data subject requests.
- **Consent**: Where required, we process your data based on your consent, such as for certain marketing communications or cookies. You may withdraw your consent at any time by following the instructions provided or by contacting us using the details in the “Contact Us” section of this Notice.

**International Data Transfers**

SonarSource is organized as a corporate group, with its parent holding company domiciled in the United States. SonarSource Sàrl, based in Switzerland, serves as the principal operating entity and is primarily responsible for processing personal data. The SonarSource group operates globally through offices and affiliates in the European Union, United Kingdom, Switzerland, Japan, Singapore, United Arab Emirates, and the United States. To provide our Sites, Services, and support, your personal data may be stored and processed in these jurisdictions and in other countries where SonarSource Sàrl, its affiliates, or authorized processors or subprocessors maintain operations.

Some of these jurisdictions may not offer the same level of data protection as your home jurisdiction. When transferring personal data from the EEA, UK, or Switzerland to countries without an adequate data protection decision—including transfers to the United States—we implement appropriate safeguards such as Standard Contractual Clauses (SCCs), UK International Data Transfer Agreements (IDTAs), Swiss Addenda, and supplementary measures as required by applicable data protection laws. We regularly review and update our data transfer mechanisms to ensure compliance with applicable laws and protection of your rights.

**Your Privacy Rights**

Depending on your location and applicable data protection laws, you may have certain rights regarding your personal data. These rights may include:

- **Right to Access**: Request information about the personal data held.
- **Right to Correction**: Correct inaccurate or incomplete personal data.
- **Right to Deletion/Erasure**: Delete or erase personal data, subject to certain exceptions (such as legal or security requirements).
- **Right to Restrict Processing**: Restrict the processing of personal data under certain circumstances.
- **Right to Object**: Object to certain processing activities, as permitted by applicable data protection laws.
- **Right to Withdraw Consent**: Withdraw consent where processing is based on consent.
- **Right to Data Portability**: Receive personal data in a structured, commonly used, and machine-readable format to facilitate transfer to another company, where technically feasible.

You may also have the right to lodge a complaint with your local Data Protection Authority. For more information, visit the European Data Protection Board site if you are an EU resident, the Swiss Federal Data Protection Commissioner's site if you are a Swiss resident, or the UK Information Commissioner's Office site if you are a UK resident.

To exercise your rights, please contact us at internal.secgov@sonarsource.com. If you are making a request on behalf of someone else, please ensure you have the necessary authorization as required by law. We may need to verify your identity before processing your request.

We respond to requests as required by law and may retain certain data to comply with legal obligations or for legal claims. For individuals in the EU, Switzerland, or the UK, we will respond to your request within one month of receipt. If necessary, and as permitted by law, we may extend this period by up to two additional months, in which case we will inform you of the extension and the reason for the delay.

**California Mandatory Disclosures**

**1. Categories of Personal Information Collected**

In the past 12 months, we have collected the categories of personal information described in the "What Information We Collect" section of this Notice. These include:

- Identifiers and contact details (such as name, email address, mailing address, phone number, user ID).
- Payment and billing information.
- Commercial information (such as transaction history).
- Internet or other electronic network activity (such as device information, browsing activity, and usage data).
- Geolocation data (general location inferred from IP address).
- Audio, electronic, visual, or similar information (such as recordings of product or user experience (UX) research calls, sales presentations, screenshots, or video submissions, where permitted by applicable data protection laws).
- Inferences drawn from the above (such as preferences or characteristics).

We collect personal information directly from you, automatically through your use of our Sites and Services, and from third parties, as outlined in "What Information We Collect."

**2. Business or Commercial Purposes for Collection**

We use personal information for the purposes described in “How We Use Your Information,” including providing, maintaining, and improving our Sites and Services, communicating with you, personalizing your experience, supporting marketing activities, ensuring security, and meeting legal obligations.

**3. Disclosure of Personal Information**

In the past 12 months, we have disclosed the categories of personal information listed above for business purposes to service providers, business partners, affiliates, and other third parties, as described in “How We Disclose Your Personal Data.”

**4. Sharing and Sale of Personal Information**

As defined by California law, we have “shared” (for cross-context behavioral advertising) and “sold” the following categories of personal information in the past 12 months: identifiers/contact information, Internet or other electronic network activity information, and inferences drawn from the above. These categories may be shared or sold to advertising networks, analytics providers, and social networks to support marketing, advertising, audience measurement, and other commercial purposes. You may opt out of this sharing by clicking the “Do Not Sell or Share My Personal Information” link in the footer of our website or by using the GPC signal, if available (as further set out in the “Cookies and Similar Technologies” section of this Notice.

We do not “sell” or “share” the personal information of known minors under 16 years of age.

**5. Your Rights and Choices**

California residents have the following rights regarding their personal information:

- **Right to Know (Access)**: Request details about the personal information we collect, use, disclose, sell, or share about you.
- **Right to Know Data Recipients**: Obtain detailed information about the specific types and categories of personal information collected over the past 12 months, including data disclosed for business purposes and the recipients of such data.
- **Right to Deletion**: Request deletion of personal information collected from you, subject to certain exceptions.
- **Right to Correct**: Request correction of inaccurate personal information maintained about you.

- **Right to Opt Out of Sale or Sharing**: Opt out of the sale or sharing of personal information for cross-context behavioral advertising.
- **Right to Non-Discrimination**: Protection from discrimination for exercising privacy rights.
- **Right to a Timely Response**: Receive a response to your request within 45 days of receipt. If we require more time, we will notify you of the reason and may extend the response period by up to an additional 45 days, as permitted by applicable data protection laws. You may submit up to two free requests within a 12-month period.

**6. Additional California Rights and Disclosures**

- **California "Shine the Light" Disclosure**: California residents may request information regarding the disclosure of their personal information to third parties for those third parties' direct marketing purposes, as defined by California Civil Code section 1798.83. To make such a request, please contact us using the information provided in the "Contact Us" section of this Notice.

**Updates to this Notice**

SonarSource may non-materially update this Notice from time to time to reflect changes in our practices, legal requirements, or the features of our Sites and Services. Any updates will be posted on our Sites, along with the date of the latest revision. We encourage you to review this Notice periodically to stay informed about how we protect your personal data. Where required by law, we will provide additional notice of significant changes. Your continued use of our Sites and Services following any non-material updates constitutes your acknowledgment and understanding of the revised Notice.

**Contact Us**

If you have any questions or concerns regarding our data practices or this Notice, or if you would like to exercise any of your privacy rights, please contact us at internal.secgov@sonarsource.com. When reaching out, please include your country and/or state of residence to help us respond appropriately.

If you are located in the United States, you may also contact us at 1 737 263 2279.

You may also opt out of certain data processing activities or withdraw your consent at any time, where applicable, by contacting us through the methods listed above.