

Privacy Policy

SCOPE

MapR Technologies, Inc. (“MapR or “we”) respects the privacy of our customers, business partners, and visitors to our websites who may provide Personal Data or data to us, and we recognize the need for appropriate protections and management of such Personal Data and data.

This Privacy Policy applies to information and data collected by MapR through its products or services and website(s) (located at: *.mapr.com). This Policy covers how MapR treats information about you that MapR collects and receives, including information related to your use of MapR products and services. This Policy does not cover data from which individual persons cannot be identified or situations in which pseudonyms are used. (The use of pseudonyms involves the replacement of names or other identifiers with substitutes so that identification of individual persons is not possible).

From time to time, MapR may offer products and services that involve additional privacy-related issues. Please check the product page of our websites for information on any such additional privacy-related issues. If there are contradictions between this Privacy Policy and the more specific information on a product page, then the latter shall prevail.

RESPONSIBILITIES AND MANAGEMENT

MapR will maintain, monitor, test, and upgrade information security policies, practices, and systems to assist in protecting the Personal Data that it collects. MapR personnel will receive training, as applicable, to effectively implement this Policy.

COLLECTION AND USE OF PERSONAL DATA

You may provide Personal Data to us when you visit the MapR Websites, join the MapR community, sign-up for one of our mailing lists, request news and product information, complete surveys, request technical support, apply for a job or job alerts, email us or purchase, download or install MapR products and services.

MapR does not sell or rent your Personal Data to anyone. We may only release Personal Data when we believe that it is required to comply with the law, or to protect the rights, property, or safety of MapR, our users, or others. This may include exchanging information with other companies and organizations for purposes of fraud protection and credit risk management. Please note, MapR mailing lists may be archived by several third party sites and your email address may be found on these archive sites. MapR doesn't have control over mailing list archive sites.

MapR collects tracking or usage data when users visit the MapR Websites, open one of

our HTML emails, (including page views, traffic flows, search terms, click throughs, Internet Protocol address, web browser type, websites visited before or after the MapR Websites and dates and times of your visits), or download or install MapR products or services (including install status (success/error), installer id, license level, services installed, cluster id, number of nodes installed). As part of our approach to providing personalized services on the MapR Websites, MapR uses cookies to store and sometimes track information about you. A cookie is a small data file sent to your browser from a web server and stored on your hard drive. The cookie remains even after you close your browser and allows easier access the next time the same page is visited. For example, a cookie is sent when you sign-up or login to the MapR Websites. With your consent, cookies can store Personal Data from forms you fill out to create a user profile so that you do not have to re-enter the information each time you visit. If you do not want your Personal Data to be stored by cookies, you can configure your browser so that it notifies you whenever a cookie is received. This way you can decide each time to accept cookies or not. However, the use of cookies may be necessary to receive certain features on the MapR Websites and choosing to reject cookies may reduce the functionality of the MapR Websites. Your browser should include precise instructions explaining how to disable or control the acceptance of cookies.

MapR uses the information that we collect for carefully considered and specific purposes which are in our interest and enable us to provide to you all of the features and services found on the MapR Websites, products and services, to create new features and functionality and to improve the way the MapR Websites, products and services work and look, for diagnostics, and to fulfil our contractual obligations to you or your employer under contract, such as an employment agreement or a software license or services agreement.

MapR may also use your Personal Data: (a) for non-promotional or administrative purposes such as notifying you of major site updates, and (b) to send promotional related communications to you unless you opt-out of receiving such communications. MapR does not sell or rent your Personal Data to anyone. We may release Personal Data when we believe that it is required to comply with the law, or to protect the rights, property, or safety of MapR, our users, or others or if you request that we release such information. This may include exchanging information with other companies and organizations for purposes of fraud protection and credit risk management.

MapR may disclose both Personal Data and automatically collected information to third party businesses, organizations or persons to process such information on our behalf, to provide website maintenance and security, to offer certain features on the MapR Websites, to assist us in improving the way the MapR Websites, products and services work and look, and/or to create new features. Please note, MapR mailing lists may be archived by third party sites and your email address may be found on these archive sites. MapR doesn't have control over mailing list archive sites.

We use automatically collected information to monitor aggregate usage metrics, trends

and preferences and to improve the MapR Websites, products and services. We may also share this anonymous traffic and demographic information in aggregate form with advertisers and other business partners. We may share automatically collected and other aggregate non-personally-identifiable information with interested third parties to assist them in understanding the usage patterns for certain content, services, products, and/or functionality on the MapR Websites. We may use automatically collected information and cookies information to remember your information so that you will not have to re-enter it during your visit or the next time you visit the MapR Website.

DATA INTEGRITY AND SECURITY

MapR uses reasonable efforts to maintain the accuracy and integrity of Personal Data and to update it as appropriate. MapR has implemented physical and technical safeguards to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. For example, electronically stored Personal Data is stored on a secure network with firewall protection, and access to MapR's electronic information systems requires user authentication via password or similar means. MapR also employs access restrictions, limiting the scope of employees who have access to Customer Personal Data.

Further, MapR uses secure encryption technology to protect certain categories of Personal Data. Despite these precautions, no data security safeguards guarantee 100% security all of the time. We urge individuals to protect their personal information when using the Internet by, for example, changing passwords often, using a combination of letters and numbers and making sure to use a secure browser.

ACCESSING PERSONAL DATA

MapR personnel may access and use Personal Data only if they are authorized to do so and only for the purpose for which they are authorized.

DURATION OF STORAGE OF PERSONAL DATA

MapR will store Personal Data only as long as is necessary to perform its obligations to Customer unless a longer period is necessary to establish, exercise or defend against legal claims.

SENSITIVE DATA

MapR does not collect Sensitive Data from its Customers. No Sensitive Data should be provided to MapR by Customers.

RIGHTS OF RESIDENTS OF THE EUROPEAN UNION

The processing of Personal Data, such as the name, business address, business e-mail address, or business telephone number of a data subject that is a resident of the European Union shall always be in line with the General Data Protection Regulation

(GDPR), and in accordance with the country-specific data protection regulations applicable to MapR for Data Protection.

By means of this data protection declaration, MapR would like to inform the general public of the nature, scope, and purpose of the Personal Data we collect, use and process. Depending on the applicable lawful basis for processing of Personal Data, Data Subjects may be entitled to one or more of the following rights under the GDPR:

a) Right of confirmation

Each data subject shall have the right granted by the European legislator to obtain from the controller the confirmation as to whether or not Personal Data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may at any time contact our CIO or another employee of the controller by sending an email to privacy@mapr.com.

b) Right of access

Each data subject shall have the right granted by the European legislator to obtain from the controller free information about his or her Personal Data stored at any time and a copy of this information. Furthermore, the European legislator grants the data subject access to the following information:

- the purposes of the processing;
- the categories of Personal Data concerned;
- the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the data subject or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- where the Personal Data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether Personal Data are transferred to a third country or to an international organization. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer. If a data subject wishes to avail himself of this right of access, he or she may at any time contact our CIO or another employee of the controller by sending an email to privacy@mapr.com.

c) Right to Rectification

Each data subject shall have the right granted by the European legislator to obtain from the controller without undue delay the rectification of inaccurate Personal Data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement. If a data subject wishes to exercise this right to rectification, he or she may at any time contact our CIO or another employee of the controller by sending an email to privacy@mapr.com.

d) Right to Erasure (Right to be Forgotten)

Each data subject shall have the right granted by the European legislator to obtain from the controller the erasure of Personal Data concerning him or her without undue delay and the controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies and as long as the processing is not necessary:

- The Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent on which the processing is based according to point (a) of Article 6 (1) of the GDPR, or point (a) of Article 9 (2) of the GDPR, and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to Article 21 (1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21 (2) of the GDPR.
- The Personal Data have been unlawfully processed.
- The Personal Data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
- The Personal Data have been collected in relation to the offer of information society services referred to in Article 8 (1) of the GDPR.

If one of the above-mentioned reasons applies and a data subject wishes to request the erasure of Personal Data stored by MapR, he or she may at any time contact the controller. MapR shall promptly ensure that the erasure request is complied with

immediately.

Where MapR has made the Personal Data public and is obliged pursuant to paragraph 1 to erase the Personal Data, MapR, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other controllers which are processing the Personal Data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those Personal Data, as far as processing is not required. The CIO of MapR or another employee will arrange the necessary measures in individual cases.

e) Right of Restriction of Processing

Each data subject shall have the right granted by the European legislator to obtain from the controller restriction of processing where one of the following applies:

- The accuracy of the Personal Data is contested by the data subject, for a period enabling the Controller to verify the accuracy of the Personal Data.
- The processing is unlawful and the data subject opposes the erasure of the Personal Data and requests instead the restriction of their use instead.
- The controller no longer needs the Personal Data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
- The data subject has objected to processing pursuant to Article 21 (1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the abovementioned conditions is met and a data subject wishes to request the restriction of the processing of Personal Data stored by MapR, he or she may at any time contact our CIO or another employee of the controller by sending an email to privacy@mapr.com. The CIO of MapR or another employee will arrange the restriction of the processing.

f) Right to Data Portability

Each data subject shall have the right granted by the European legislator, to receive the Personal Data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the Personal Data have been provided as long as the processing is based on consent pursuant to point (a) of Article 6 (1) of the GDPR or point (a) of Article 9 (2) of the GDPR or on a contract pursuant to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official

authority vested in the controller.

Furthermore, in exercising his or her right to data portability pursuant to Article 20 (1) of the GDPR, the data subject shall have the right to have the Personal Data transmitted directly from one controller to another, where technically feasible and does not adversely affect the rights and freedoms of others.

In order to assert the right to data portability, the data subject may at any time contact the CIO designated by MapR or another employee by sending an email to privacy@mapr.com.

g) Right to Object

Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time to processing of Personal Data concerning him or her which is based on point (e) or (f) of Article 6 (1) of the GDPR. This also applies to profiling based on these provisions.

MapR shall no longer process the Personal Data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

If MapR processes Personal Data for direct marketing purposes, the data subject shall have the right to object at any time to processing of Personal Data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to MapR to the processing for direct marketing purposes, MapR will no longer process the Personal Data for these purposes.

In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of Personal Data concerning him or her by MapR for scientific or historical research purposes or statistical purposes pursuant to Article 89 (1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may directly contact the CIO of MapR or another employee by sending an email to privacy@mapr.com. In addition, the data subject is free in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

h) Automated individual decision-making in specific case, including profiling

Each data subject shall have the right granted by the European legislator not to be

subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, as long as the decision (1) is not necessary for entering into, or performance of, a contract between the data subject and a data controller, or (2) is not authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or (3) is not based on the data subject's explicit consent.

If the decision (1) is necessary for entering into, or performance of, a contract between the data subject and a data controller, or (2) it is based on the data subject's explicit consent, MapR shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may at any time directly contact our CIO of MapR or another employee of the Collector by sending an email to privacy@mapr.com.

i) Right to withdraw data protection consent

Each data subject shall have the right granted by the European legislator to withdraw his or her consent to processing of his or her Personal Data at any time. If the data subject wishes to exercise the right to withdraw the consent, he or she may at any time directly contact our CIO of MapR or another employee of the controller by sending an email to privacy@mapr.com.

j) Legal basis for processing

MapR processes Personal Data with your consent, when necessary for the performance of an agreement with you or when we have another legitimate and justifiable interest in processing your Personal Data, such as an interest in marketing ourselves to visitors to our website or an interest in developing our website or our products and/or services. If we were to process your personal data for any purpose which, according to applicable legislation, requires your consent, we will obtain your consent before commencing with such processing.

ONWARD TRANSFERS OF PERSONAL DATA

Except as otherwise provided herein, MapR discloses Personal Data only to Third Parties who reasonably need to know such data only for the scope of the initial transaction and not for other purposes. Such recipients must agree to abide by confidentiality obligations.

MapR may provide Personal Data to Third Parties that act as agents, consultants, and contractors to perform tasks on behalf of and under our instructions. For example, MapR may store such Personal Data in the facilities operated by Third Parties. Such Third Parties must agree to use such Personal Data only for the purposes for which they have been engaged by MapR. When Personal Data of residents of the European Union is provided to Third Parties, such Third Parties must either comply with mechanism permitted by the applicable EU & Swiss data protection law(s) for transfers and processing of Personal Data or agree to provide adequate protections for the Personal Data that are no less protective than those set out in this Policy.

MapR also may disclose Personal Data for other purposes or to other Third Parties when a Data Subject has consented to or requested such disclosure. Please be aware that MapR may be required to disclose an individual's Personal Data in response to a lawful request by public authorities, including to meet national security or law enforcement requirements. MapR is liable for appropriate onward transfers of Personal Data

YOUR CALIFORNIA PRIVACY RIGHTS

Residents of the State of California, under California Civil Code § 1798.83, have the right to request from companies conducting business in California a list of all third parties to which the company has disclosed personal information during the preceding year for direct marketing purposes. Alternatively, the law provides that if the company has a privacy policy that gives either an opt-out or opt-in choice for use of your personal information by third parties (such as advertisers) for marketing purposes, the company may instead provide you with information on how to exercise your disclosure choice options.

MapR qualifies for the alternative option. We have a comprehensive privacy statement, and provide you with details on how you may either opt-out or opt-in to the use of your personal information by third parties for direct marketing purposes. Therefore, we are not required to maintain or disclose a list of the third parties that received your personal information for marketing purposes during the preceding year.

If you are a California resident and request information about how to exercise your third party disclosure choices, please email us your request to privacy@mapr.com

THIRD PARTY SITES

MapR websites may provide links to other third party websites which are outside of our control and not covered by this Policy. We encourage you to review the privacy policies posted on such third party websites.

IN THE EVENT OF MERGER OR SALE

If MapR should have its assets sold to or merge with another entity, information MapR

receives from you through the MapR Websites is a MapR asset and may be transferred.

SPECIAL NOTE TO INTERNATIONAL USERS

The MapR Websites are hosted in the United States. If you are a user accessing the MapR Websites from the European Union, Asia, or any other region with laws or regulations governing Personal Data collection, use, and disclosure that differ from United States laws, please note that you are transferring your Personal Data to the United States which does not have the same data protection laws as the EU and other regions and by providing your Personal Data you consent to: (1) the use of your Personal Data for the uses identified above in accordance with this Policy; and (2) the transfer of your Personal Data to the United States as indicated above.

CHILDREN AND PRIVACY

Our Websites do not target and are not intended to attract children under the age of 13. MapR does not knowingly solicit personal information from children under the age of 13 or send them requests for personal information.

CHANGES TO THIS POLICY

If we change the Policy, we will post an updated privacy policy at www.mapr.com/privacy. If we decide to use Personal Data in a manner different from that stated at the time it was collected, we will notify users via email. Customers will be able to opt out of any new use of their Personal Data. We encourage you to periodically review this Privacy Statement to stay informed about how we are protecting the Personal Information we collect. Your continued use of the MapR Websites constitutes your agreement to this Privacy Statement and any updates.

DEFINED TERMS

Capitalized terms in this Privacy Policy have the following meanings:

"Customer" means a Customer or client of MapR from EU or Switzerland. The term also shall include any individual agent, representative, of a Customer of MapR and all employee of MapR where MapR has obtained his or her Personal Data from such customer as part of its business relationship with MapR.

"Data Subject" means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics. For Customers residing in Switzerland, a Data Subject also may include a legal entity.

"Employee" means an employee (whether temporary, permanent, part-time, or contract), former employee, independent contractor, or job applicant of MapR or any of its affiliates or subsidiaries, who is also a resident of a country within the European Economic Area.

"Europe" or "European" refers to a country in the European Union.

"Personal Data" as defined under the European Union Directive 95/46/EC means data that personally identifies or may be used to personally identify a person, including an individual's name in combination with country of birth, marital status, emergency contact, salary information, terms of employment, job qualifications (such as educational degrees earned), address, phone number, e-mail address, user ID, password, and identification numbers. Personal Data does not include data that is de-identified, anonymous, or publicly available.

"Sensitive Data" means Personal Data that discloses a Data Subject's medical or health condition, race or ethnicity, political, religious or philosophical affiliations or opinions, sexual orientation, or trade union membership.

"Third Party" means any individual or entity that is neither MapR nor an MapR employee, agent, contractor, or representative.