Tribe

Processing conditions for Tribe CRM of PerfectView B.V.

Contents

Tribe

Processing conditions for Application Software for Tribe CRM of PerfectView B.V.

1. The private company with limited liability PerfectView B.V. has its registered office in Rijswijk and its place of business in (5215MX) 's-Hertogenbosch at De Waterman 2, registered with the trade register under number: 27247845, hereto legally represented by Mrs K.I. Alleijn in the position of operational director, hereinafter referred to as "Processor";

and

2. The client (as defined in the general terms and conditions and as described in the (Partner) application, application, quotation, order confirmation or similar agreement) is the (legal) person or organisation that has given a digital or written order to Processor for the supply of Software, services or other items, hereinafter referred to as "Controller";

Jointly referred to as "Party or Parties";
Whereas:

- The Controller intends to have certain types of processing performed by the Processor, while the Controller determines the purpose and means;
- The Processor is prepared to accept this order and is also prepared to comply with obligations regarding security and other aspects of the General Data Protection Regulation and any related regulations and codes of conduct;
- The Parties have concluded one or more agreements ("Agreement(s)") in which the processing of personal data forms part of the service provision;
- Partly in view of the requirements of Article 28, third paragraph, of the GDPR, the Parties wish to lay down their rights and obligations in these Processing Conditions;
- Where in these Processing Conditions terms are used that correspond with definitions from Article 4 of the GDPR, these terms are assigned the meaning of the definitions provided in the GDPR.

Controller and Processor agree as follows:

1. Definitions

Appendices: Appendices to these Processing Terms and Conditions that form part of

these Processing Terms and Conditions.
Supervisor: the Personal Data Authority (Autoriteit Persoonsgegevens, AP) is the independent administrative body appointed by law in the Netherlands to supervise the processing of personal data.
Controller: a natural or legal person, a government body, a service or other body which, alone or jointly with others, determines the purpose of and means of processing personal data.
Processor: a natural or legal person, a government body, a service or other body that processes personal data on behalf of Controller. The person who processes personal data on behalf of Controller, at the instructions of Processor, is a sub-processor.

2. Effective date and duration

2.1. These Processing Conditions commence from the conclusion of the Agreement and continue to be effective for as long as the Processor acts as a Processor of personal data with respect to the personal data provided by the Controller for processing on the Processor's platform.

3. Subject of these Processing Terms and Conditions

3.1. Processor processes the personal data made available by or via the Controller exclusively on the instructions of the Controller in the context of the execution of the main agreement. The activities to be performed by Processor to which these Processing Conditions relate are further described in Appendix 2. The Processor will not process the personal data for any other purpose, except for deviating statutory obligations.

3.2. Processor undertakes to carefully process the personal data provided by or via Controller with respect to these activities.

4. Obligations of the Processor and the Controller

4.1. The Processor processes data on behalf of Controller in accordance with its (written) instructions.

4.2. The Controller guarantees Processor that the processing of personal data is lawful. If Processor is of the opinion that Processor is acting in violation of the GDPR, the Processor will notify the Processor accordingly.

4.3. The Processor has no control over the personal data provided. For example, it does not make decisions about the receipt and use of the data, the provision to third parties and the duration of data storage. The control over the personal data provided under these Processing Conditions is not and will not be vested with the Processor.

4.4. When processing personal data with respect to the activities referred to in Article 3, the processor will act in accordance with the applicable laws and regulations concerning the processing of personal data. The Processor will follow all reasonable instructions of (the contact person of) the Controller, subject to deviating legal obligations. If such deviating legal obligations exist, the Processor will inform the Controller in writing prior to processing.

4.5. The Processor shall at all times enable the Processor to comply with the obligations under the GDPR within the statutory time limits, in particular the rights of data subjects, such as, but not limited to, a request to inspect, correct, supplement, delete or discard personal data and to execute an accepted objection. The reasonable associated costs will be borne by the Controller.

4.6. The Processor will cooperate with a data protection impact assessment ((D)PIA) at all times upon request of the Processor. The reasonable associated costs shall be borne by the Controller.

5. Duty of confidentiality

5.1. Persons employed by or working on behalf of Processing Company, as well as the Processing Company itself, are obliged to observe confidentiality with respect to the personal data which they may take note of, except to the extent that an obligation to provide such data is imposed by or pursuant to the law. To this end, the employees of the Processor are obliged to observe secrecy.

5.2. If the Processor has a legal obligation to provide data to a third party, the Processor will verify the basis of the request and the identity of the applicant and will inform the Controller immediately prior to such supply of data, unless this is prohibited by legal provisions.

6. Duty to report data breaches and security incidents

6.1. The Processor shall inform the Controller as soon as possible - in relation to the term applicable to any reporting obligation of the Controller - of all relevant breaches of security, without prejudice to the obligation to undo or limit the consequences of such breaches and incidents as soon as possible. In doing so, if possible, the Processor shall provide the information to the Controller as described in Appendix 3.

6.2. The Processor has a solid plan of action concerning the handling and settlement of infringements and will, at the request of the Processor, provide the Processor with access to the plan.

6.3. The Processor is not obliged to report to the Supervisor. This responsibility is vested with the Controller.

6.4. If necessary, the Processor will provide the Supervisor and/or person(s) concerned with additional information as soon as possible. In doing so, the Processor shall in any case provide the information as described in Appendix 3 to the Controller.

6.5. The Processor keeps a record of all (suspected) breaches of security, as well as the action taken in response to such breaches.

7. Security measures and control

7.1. The Processor shall take all appropriate technical and organisational measures to secure the personal data being processed for the purposes of the Controller and to keep them secure against loss or against any form of unlawful processing. The protection method is specified in Appendix 1.

7.2. The person responsible is entitled to check, or cause to check, the processing of personal data by independent experts working under secrecy, however, no more than once a year.

7.3. The Controller will only conduct (or cause to conduct) the verification after a prior written notification to the Processor and after existing reports of the Processor have been assessed as insufficient.

7.4. Within a reasonable period of time of at least two weeks, the Processor shall provide the Controller, or the third party engaged by the Controller, with the requested information. As a result, the Controller, or the third party engaged by the Controller, may form an opinion on compliance by the Processor with these

Processing Conditions. The Controller, or the third party engaged by the Controller, is obliged to treat all information relating to these checks as confidential.

7.5. The Processor guarantees to implement the appropriate measures for improvement indicated by the Controller or hired third party within the reasonable period of time to be determined by the Controller.

7.6. In addition to reports from the Processor and audits by the Controller or control body on behalf of the Controller, both parties may also agree to make use of an ISO 27001 certification drawn up by an independent external expert.

7.7. The costs of the audit shall be borne by the party who incurs the costs.

8. Engagement of third parties

8.1. The Processor lists the third parties known at the time of the conclusion of the Agreement who process personal data for the Processor in Appendix 4. The Controller hereby gives general permission for the engagement of third parties. After the start of the work, the Processor shall keep the Controller informed of the engagement of new third parties.

8.2. The Processor guarantees that these third parties will assume sufficient obligations in writing as agreed between the Controller and the Processor and will, at the latter's request, allow the Controller to inspect the agreements with these third parties in which these obligations are included.

8.3. The Processor may only process personal data within the European Economic Area (EEA). Transfer to other countries outside the EEA is only permitted with the prior written consent of the Controller and subject to applicable laws and regulations.

8.4. The Processor shall keep an up-to-date register of the third parties and subcontractors engaged by it in which the identity, place of business and a description of the activities of the third parties or subcontractors are included, as well as any additional conditions set by the Controller. This register will be added as Appendix 4 to these Processing Conditions and will be kept up to date by the Processor.

9. Modification and termination Processing terms and conditions

9.1. The Processor is entitled to make changes to the Processing conditions. The Controller will then be given thirty days to let the Processor know if he does not agree. Without notice to the contrary from the Controller, the changes will be considered as accepted by the Controller.

9.2. Upon termination of the agreement as described in the CRM Online terms and conditions, (i) the Processor will provide to the Controller all personal data provided under these Processor terms and conditions, in accordance with the provisions of the CRM Online terms and conditions regarding the extraction of personal data for this purpose (ii) the Processor will destroy the personal data received from the Controller at all locations, in any form whatsoever, unless mandatory provisions require that certain data must be retained. The associated reasonable costs shall be borne by the Processor.

9.3. The Processor will at all times guarantee the right to transfer data as described in the previous paragraph in accordance with Article 20 of the GDPR in such a way that there is no question of loss of (parts of) the data.

9.4. The Processor will inform the Controller in a timely manner about changes to these Processing Terms and Conditions, if a change to regulations or a change in the interpretation of regulations gives cause to do so.

9.5. If a Party fails to perform an agreed obligation, the other Party may issue a notice of default, allowing the defaulting Party a reasonable period of time to perform. If the defaulting Party nonetheless fails to comply, the defaulting Party shall be in default. Notice of default is not necessary if performance is subject to a strict deadline, performance is permanently impossible or if it must be inferred from a notification or the attitude of the other party that it will fail in the performance of its obligation.

9.6. Without prejudice to the provisions to that end in the Processing Conditions and the main agreement associated therewith, and without prejudice to the other provisions of the law, the Controller is entitled to suspend the execution of these Processing Conditions through a registered letter, or to dissolve these Processing Conditions in whole or in part with immediate effect without judicial intervention, after the Controller becomes aware that:

(a) the Processor applies for (provisional) suspension of payment; or
(b) the Processor files for bankruptcy or is declared bankrupt; or
(c) the Processor's company is dissolved; or
(d) the Processor ceases his business; or
(e) in case of a substantial change in the control over the activities of the company of the Processor that makes it unreasonable to expect the Controller to maintain the Processing conditions; or
(f) a substantial part of the assets of the Processor are seized (other than by the Controller); or
(g) the Processor fails to comply with the obligations arising from these Processing Conditions and this attributable shortcoming has not been remedied within 30 days following a written notice of default to that effect or one of the other situations referred to in Article 9.5 occurs.

9.7. In the event of early termination of the Agreement(s), Article 9, paragraphs 2 and 3 shall apply mutatis mutandis.

10. Liability

10.1. The Processor is liable pursuant to the provisions of article 82 of the GDPR for direct damage resulting from failure to comply with these Processing conditions, including if the processing does not comply with the obligations of the GDPR specifically addressed to the Processor, or if action has been taken outside the lawful instructions of the Controller.

10.2. The Processor shall only be liable for direct damage to the extent it is caused by the activity of the Processor. Any liability on the part of PerfectView shall be limited per event, whereby a coherent series of events shall be regarded as a single event, to the amount paid out by PerfectView's corporate liability insurer. If the insurer does not pay out for any reason, the liability of PerfectView per event, whereby a coherent series of events counts as one event, is limited to the amount equal to the price of the Assignment, which was invoiced in the period of 12 months immediately preceding the event causing the damage.

10.3. Direct damage is understood to be limited to the loss items included in the policy sheets of PerfectView's liability insurance.

10.4. Liability for trading losses, including losses due to loss of profit or non-achieved savings, damage to reputation or other indirect or consequential loss is excluded. Also PerfectView's liability in connection with the mutilation, destruction or loss of

data or documents is excluded, for example in the event of a security incident and/or data breach, or the prevention or limitation thereof.

10.5. The above limitations of liability shall lapse in the event of intent or gross negligence on the part of PerfectView and/or its executive subordinates.

10.6. If the Processor fails to comply with the obligation laid down in Article 6 paragraph 1 of these Processing Conditions or fails to do so on time and the Supervisor consequently imposes an administrative fine on the Processor, the Processor shall be liable and the Controller shall impose a contractual fine of the same amount on the Processor. This fine is not subject to any set-off and suspension and does not affect the rights of the Controller to compliance and compensation.

10.7. If the Processor receives a sanction imposed by the Supervisor or is required to compensate a data subject for damages as a result of acts or omissions by the Controller, the Controller shall indemnify the Processor and compensate the latter at its first request for this sanction or damage, including (legal) costs.

11. Applicable law

11.1. These Processing Conditions and all respective disputes arising from or related to the Processing Conditions shall be governed exclusively by Dutch law.

11.2. All disputes arising in relation to this Processing Agreement shall be settled in the same manner as provided in the Agreement, which the General Terms and Conditions of PerfectView B.V. form part of.

11.3. In addition to these Processing Conditions, the Terms and Conditions for CRM Online apply. In case of any discrepancies between the various documents, the order is as follows: (1) Agreement (2) Licence terms for CRM Online (3) the Processor terms for CRM Online (4) Terms and conditions for CRM Online (5) Privacy statement.

Tribe

Appendices

Appendix 1: Description of security measures

For the purposes of Article 7, paragraph 1

Appendix 2: Description of Processor's activities

For the purposes of Article 3, paragraph 1

Appendix 3: Information to assess incidents

For the purposes of Article 6, paragraphs 1 and 5

Appendix 4: Sub-processor register

For the purposes of Article 8, paragraphs 1 and 5

Tribe

Annex 1: Description of security measures for Tribe CRM

For the definition of the terms used, reference is made to the Tribe CRM processing conditions of PerfectView B.V.

This document explains in detail the organisational and technical security measures of the Tribe CRM Application Software. The focus is mainly on the measures aimed at the continuity, integrity and availability of the Application Software Tribe CRM.

Since personal data is processed in the Tribe CRM application, these measures are essential in order to achieve an appropriate level of security as required by the GDPR for data processors (GDPR Article 28).

Organisational measures

ISO 27001 certification

PerfectView is ISO 27001:2013 certified. PerfectView works very actively throughout the organisation to ensure optimal information security. The certification is assessed annually by an independent accredited body. The hosting partner Google, which serves as subprocessor, is ISO 27001, ISO 270017, ISO 27018 and SSAE 16/ISAE 3402 Type II certified.

EEA (European Economic Area)

Both PerfectView and all storage sites that together offer the Tribe CRM application are located in the EEA. For the hosting we only use the physical Google locations in the EEA (Including data centres in Eemshaven in the Netherlands and in Saint-Ghislain in Belgium) and are fully compliant with EU data protection legislation.

Reporting

PerfectView shares information about the measures and results of audits and pen tests relating to information security with the security officer via news items in the application, and via e-mail messages specifically to the security officer.

Partners

PerfectView utilises a select group of subprocessors who, like PerfectView, consider availability, integrity and confidentiality equally important. Agreements are laid down in binding processor agreements and service level agreements.

Responsibilities

All employees of PerfectView have signed a non-disclosure statement in respect of all information they become aware of. A Certificate of Good Conduct (Verklaring Omtrent het Gedrag, VOG) has been and is periodically requested from all employees for the tasks applicable to their position.

Periodically, all employees are informed about their responsibilities with regard to information security. Employees only have the minimum access rights required for the performance of their duties.

A Chief Information Security Officer and a Data Protection Officer have been appointed within PerfectView.

Development

Security aspects (availability, integrity and confidentiality) constitute an integral part of design, development and testing. Changes are implemented in the various environments in a controlled manner.

Tribe

Technical measures

Internet communication

The connection between the Tribe CRM application in the data centre and the Internet is redundant. Connections have been set up from the data centre to multiple internet nodes in the Netherlands.

Communication with our Tribe CRM application is encrypted during transmission. The network and infrastructure have multiple layers of security to protect our customers against DoS (Denial of Service) attacks.

The balanced network traffic is limited to only the necessary services, port HTTP (port 80) and HTTPS (port 443) for the web services and SMTP (port 25) for the mail services are allowed in the firewall routes.

The routes can only lead to servers that actually offer the services. Internet access to the environment does not allow access for technical management or direct access to the database systems.

Storage

Data stored in our infrastructure is automatically encrypted on the server and distributed for availability and reliability. In this way, we protect your information from unauthorized access and service interruptions.

Infrastructure

The infrastructure in the data centre is completely redundant. All connections on the public (internet) side as well as on the local management side are redundant. The linked network components such as network switches, firewalls and load balancers are also redundant.

From the physical location to the purpose-built servers, network equipment, custom security chips and low-level software stack running on each computer, the entire hardware infrastructure is managed, secured, designed and reinforced by Google.

The different environments for development, testing, acceptance and production are set up completely separately.

Data centres

PerfectView takes advantage of Google's data centres, using a layered security model with specially designed electronic access passes, alarm systems, barriers, fences, metal detectors and biometric systems. The floor of the data centres is protected against intruders with laser detection.

The data centres are secured 24 hours a day by high-resolution indoor and outdoor cameras that can detect and track intruders. Only authorised employees with specific roles have access to the data centres.

Updates

The environment is periodically updated with service updates from the suppliers. The updates for the infrastructure, storage systems and cloud services are performed by Google. The Tribe CRM application systems are kept up to date by PerfectView. PerfectView uses a continuous delivery process in the DevOps teams to develop its application quickly and efficiently. This allows adjustments to be implemented in the product in a short cyclical manner.

Backups

All data is backed up every night. The backups are placed in a separate backup environment and kept there for a period of 3 months. The backups are stored encrypted.

Total backup retention is 3 months. Deletion of (personal) data will take place a.s.a.p. at the request of the person in charge but will only lead to complete destruction after the end of the backup cycle.

Anti-virus

All servers and (management) workstations are equipped with anti-virus software which is updated daily.

E-Mail

All outgoing email is routed through anti-spam/antivirus filters to prevent/stop unwanted messages. PerfectView closely monitors mail traffic. Flowmailer's mail platforms are used for this purpose.

Communication

Data is only exchanged via cryptographically secured connections. All communication between clients (users) and the servers is encrypted via SSL. PerfectView uses an SSL certificate with an SSL 2048 bit SHA 265 key.

Monthly checks are made to see if the certificates, chipers and keys that are being used still score an A Grade in the tests of SSLLabs.com to see if there is sufficient cryptographic protection active.

Penetration test

At least once a year, the Tribe CRM application is extensively tested for vulnerabilities. A so-called black and grey penetration test is performed by an independent organisation based on OWASP best practices. PerfectView can provide the cover letter of the latest pen test on request.

Access security

User access is possible on the basis of complex passwords. Complexity and change policy of passwords can be set by the application administrator. We do not store user passwords. PerfectView uses irreversible encryption, which immediately converts passwords into a code (hash) that cannot be decrypted by third parties.

After 3 unsuccessful login attempts within 5 minutes, an account is blocked for a certain period of time so that no one can try to crack a password forever.

Application administrators can additionally specify IP addresses in the application settings, from which they can and may log in.

Access to the data for PerfectView is limited to the support staff of PerfectView designated by the customer. Employees of PerfectView will never ask for confidential information such as password information by e-mail or phone.

Monitoring

The Tribe CRM application is continuously monitored in order to be able to perform maintenance, fault repair, capacity management, etc. adequately and on time.

Logging

In the Tribe CRM application, extensive audit logs are created regarding data changes and system changes by users and administrators. The logs cannot be modified or manipulated by the user and/or administrator.

Tribe

Appendix 2: Description of activities of processor Tribe CRM

For the definition of the terms used, reference is made to the Tribe CRM processing conditions of PerfectView B.V.

1. Processing

This processing register shall designate two processing operations under the contract between the processor and the responsible party.

1.1. Processing user data

Target	User administration for access to the Application Software by employees of the responsible party
Legal basis	Execution of the agreement
Those concerned	Employees of responsible
Duration	Duration of the agreement

The following Personal Data will be processed in the context of the Agreement:

- Name, email, and organisation (indirectly derivable).

Processor processes personal data for controller in the following ways:

- User data is stored for management purposes by the person responsible for access control of the Application Software.

- User data will be used to inform responsible and involved parties about changes and/or incidents in the Application Software as offered by the processor.

Responsible person determines which Personal Data is processed.

1.2. Offer Application Software

Target	Offering Application Software for the purpose of registering relationship data of the responsible party. The offering of Application Software also includes the inextricably linked processing operations such as hosting, backing up, managing, supporting and developing the Application Software.
Legal basis	Execution of the agreement
Those concerned	Relationships, employees of the registered relations and employees of the person in charge
Duration	Duration of the agreement

Within the framework of the agreement, the Software Application offers the possibility to process personal data. PerfectView assumes the following personal data and has adjusted its security measures accordingly:

- Name (call, first name, surname and insertions), gender, e-mail, website, telephone numbers (mobile, landline, skype and fax), address details (street, house number, postcode, city and country) and employer.

Processor processes personal data for controller in the following ways:

- User data is stored for the purpose of customer relationship management by the person in charge as support in the execution of its business processes.

- Data is stored, maintained and backed up on the platform in such a way that it can be accessed by the responsible party, is available during/after updates and can be restored in case of calamities.

- PerfectView does not distribute any personal data within its platform to third parties.

Responsible party determines which personal data is processed and/or the security measures offered are adequate for its processing.

Tribe

Appendix 3: Information to assess incidents for Tribe CRM

With regard to the definitions of the terms used, reference is made to the Tribe CRM processing conditions of PerfectView B.V.

Duty to report data breaches and security incidents

The processor shall provide all information deemed necessary by the controller to assess the incident. The processor shall provide the controller with information such as:

- the (alleged) cause of the infringement;
- the (as yet known and/or expected) implications;
- the (proposed) solution;
- contact details for the follow-up of the report;
- number of persons whose data is involved in the infringement (if no exact number is known: the minimum and maximum number of persons whose data is involved in the infringement);
- a description of the group of persons whose data is involved in the infringement;
- the type or types of personal data involved in the breach;
- the date on which the infringement took place (if no exact date is known: the period during which the infringement took place);
- the date and time on which the processor became aware of the infringement or a third party or subcontractor engaged by him;
- whether the data has been encrypted, hashed or otherwise made incomprehensible or inaccessible to unauthorised persons;
- the measures already taken to end the infringement and to mitigate its effects.

Tribe

Appendix 4: Tribe CRM subprocessor register

The processor shall use the sub-processors listed in this Annex in the performance of the contract. The processor shall update this appendix in accordance with article 8 of the Tribe CRM processing conditions of PerfectView B.V. in case of changes to the subprocessors engaged and shall provide this list to the controller without delay.

With regard to the definition of the terms used, reference is made to the Tribe CRM processing conditions of PerfectView B.V.

Hosting

Subprocessor	**Google Ireland Limited**
Location	Gordon House Barrow Street Dublin 4 Ireland
VAT number	IE 6388047V
Description of the activities	Hosting Tribe CRM platform including redundant utilities, infrastructure storage systems and (server) hardware, access security, firewall and anti-DDos protection. https://cloud.google.com/security/infrastructure/
Certifications	https://cloud.google.com/security/compliance/#/

Tribe

Email providers

Subprocessor	**MailJet**
Location	13 Rue De L Aubrac 75012 Paris-France
VAT number	FR67524536992
Description of the activities	Mail delivery system for sending messages and the status feedback of the messages from the Tribe CRM platform. Scanning outgoing mail streams for virus and spam content.
Certifications	ISO 27001, https://www.mailjet.com/gdpr/mailjet-first-esp-iso-27001-and-gdpr-certified/ https://www.mailjet.com/privacy-policy/