General Processing Terms and Conditions PerfectView CRM Online of Efficy Nederland B.V.

Standard Processing Terms and Conditions of PerfectView CRM Online of Efficy Nederland B.V.

1. The private company with limited liability Efficy Nederland B.V. with its registered office in ‘s-Hertogenbosch and with offices at (5215MX) 's-Hertogenbosch at De Waterman 2, registered in the Dutch Chamber of Commerce (KvK) under number: 27247845, trading under the name PerfectView, legally represented by Mrs K.I. Alline 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) registration, registration, offer, order confirmation or similar agreement) being the (legal) person or organization that has issued a digital or written instruction to the Processor for the delivery of Software, services or other matters, hereinafter referred to as "Controller";

Together referred to as “Parties”;

Taking into consideration that:

- The Controller wishes to have certain forms of processing done by the Processor, whereby the Controller indicates the purpose and the means;
- The Processor is willing to do so and is also prepared to comply with obligations regarding security and other aspects of the General Data Protection Regulation and related regulations and codes of conduct;
- The Parties have concluded one or more agreements ("Agreement (s)") in which the processing of personal data is part of the service;
- The Parties, having regard to the requirements of Article 28, third paragraph of the GDPR, wish to record their rights and obligations in these Processing Terms and Conditions;
- Where terms are used in these Processing Terms and Conditions that correspond with definitions from Article 4 of the GDPR, these terms shall be assigned the meaning of the definitions from the GDPR.

The Controller and the Processor agree to the following:

Article 1 Definitions

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

1.2 Supervisory Authority: the Dutch Data Protection Authority (AP) is the independent administrative body that has been appointed by law as a supervisory authority in the Netherlands for the supervision of the processing of personal data.

1.3 Controller: a natural or legal person, a government agency, a service or any other body that, individually or jointly with others, determines the purpose of and the means for the processing of personal data.

1.4 Processor: a natural or legal person, a government body, a service or another body that processes personal data on behalf of the Controller. The person who processes personal data on behalf of the Controller, on behalf of the Processor, is a sub-Processor.

Article 2 Inception date and duration

2.1 These Processing Terms and Conditions start at the moment of entering into the Agreement and continue for as long as the Processor acts as a Processor of personal data in the context of the personal data made available by the Controller for processing on the platform of the Processor.

Article 3 Subject of these Processing Terms and Conditions

3.1 The Processor processes the personal data made available by or through the Controller solely on the instructions of the Controller in the context of the execution of the main agreement. The activities to be performed by the Processor to which these Processing Terms and Conditions apply are described in more detail in Appendix 2. The Processor will not process the personal data for any other purpose except for deviating legal obligations.

3.2 In the context of these activities, the Processor undertakes to carefully process the personal data made available by or via the Controller.

Article 4 Obligations of Processor and Controller

4.1 The Processor processes data for the benefit of the Controller in accordance with his (written) instructions.

4.2 The Controller guarantees that the processing of personal data is lawful. If the Processor is of the opinion that the Controller acts in conflict with the GDPR, the Processor will inform the Controller accordingly.

4.3 The Processor has no control over the personal data made available. As such he does not take decisions about receipt and use of the data, the provision to third parties and the duration of the storage of data. The control over the personal data provided under these Processing Terms and Conditions shall never be vested in the Processor.

4.4 When processing personal data in the context of 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 from (the contact person of) the Controller, except for deviating legal obligations. If these deviating legal obligations exist, the Controller will be informed of this in writing by the Processor prior to processing.

4.5 The Processor shall at all times enable the Controller to comply with the obligations under the GDPR, in particular the rights of data subjects, such as, but not limited to, a request for inspection, rectification, supplementing, erasure or the protection of personal data and the execution of an honoured registered objection. All reasonable costs associated with this shall be borne by the Controller.

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

Article 5 Confidentiality

5.1 Persons employed by or employed for the benefit of the Processor, as well as the Processor himself, are obliged to maintain confidentiality with regard to the personal data of which they can take cognizance, except insofar as a provision prescribed by or pursuant to the law makes disclosure obligatory. The employees of the Processor are held to confidentiality.

5.2 If the Processor is required to provide information to a third party on the basis of a legal obligation, the Processor will verify the basis of the request and the identity of the applicant and the Processor will immediately inform the Controller before providing such information, unless legal stipulations prohibit this.

Article 6 Duty to report data leaks & security incidents

6.1 The Processor will inform the Controller as soon as possible - within the term that applies to any potential duty to report by the Controller - of all relevant security breaches, without prejudice to the obligation to undo or limit the consequences of such breaches and incidents as quickly as possible. In doing so, the Processor provides, if possible, the information to the Controller as described in Appendix 3.

6.2 The Processor has a thorough plan of action in place with regard to the handling and processing of infringements and will provide the Controller, upon his request, access to the plan.

6.3 The Processor is not obliged to submit a report to the Supervisory Authority. This responsibility rests with the Controller.

6.4 The Processor will provide all necessary cooperation to provide additional information to the Supervisory Authority and / or involved parties as necessary, in the shortest possible term. In any case, the Processor shall thereby provide the Controller with the information as described in Appendix 3.

6.5 The Processor keeps a log of all (suspected) security breaches, as well as the measures taken in connection with such breaches.

Article 7 Security measures and audits

7.1 The Processor shall take all appropriate technical and organizational measures to protect the personal data processed in the service of the Controller and to keep it protected against loss or against any form of unlawful processing. The method of security is described in more detail in Appendix 1.

7.2 The Controller is entitled to (conduct an) audit (of) the processing of personal data by independent experts working under a confidentiality agreement, but at most once a year.

7.3 The Controller will only conduct such audit (or have it conducted) after a prior written notification to the Processor and after existing reports by the Processor have been assessed as unsatisfactory.

7.4 The Processor will provide the requested information within a reasonable period of time, of a minimum of two weeks, to the Controller or to a third party engaged by the Controller. As such, the Controller or the third party engaged by the Controller can evaluate the compliance of these Processing Terms and Conditions by the Processor. The Controller or the third party engaged by the Controller is obliged to treat all information concerning these audits as confidential.

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

7.6 In addition to reports by the Processor and audits by the Controller or the controlling authority on the instructions of the Controller, both parties can also agree to use an ISO 27001 certification drawn up by an independent external expert.

7.7 The costs of the audit are borne by the party that incurs the costs.

Article 8 Third party engagements

8.1 The Processor is only entitled to outsource the execution of the work entirely or partly to third parties after prior notification of the Controller or to the extent agreed within these Processing Terms and Conditions.

8.2 The Processor guarantees that these third parties will take on sufficient obligations in writing as are agreed between the Controller and the Processor and shall provide Controller, at his request, with access to the agreements with these third parties in which these obligations are included.

8.4 The Processor may only process the personal data within the European Economic Area (EEA). Transfers to other countries outside the EEA are only permitted with the prior written consent of the Controller and with due observance of the applicable laws and regulations.

8.5 The Processor shall keep an up-to-date register of the third parties and subcontractors it has engaged, including the identity, location and description of the activities of the third parties or subcontractors as well as any additional conditions set by the Controller. This register will be added to these Processor Conditions as Appendix 4 and will be kept up to date by the Processor.

Article 9 Changes and termination of Processing Terms and Conditions

9.1 The Processor is entitled to make changes to the Processing Terms and Conditions. The Controller subsequently has thirty (30) days to express disagreement. In the absence of a counter notification by the Controller, the changes are considered to have been accepted by the Controller.

9.2 As soon as the cooperation is terminated, the Processor will, at the choice of the Controller, (i) make available to the Controller all of the personal data made available within the framework of these Processing Terms and Conditions (ii) destroy the personal data he has received from the Controller at all locations, in any form whatsoever, and demonstrate proof of this, unless the parties agree otherwise. This work must be carried out within a reasonable term to be agreed upon. The associated reasonable costs will be borne by the Processor.

9.3 The Processor will at all times guarantee the right to transfer data in accordance with Article 20 of the GDPR as described in the previous paragraph in such a way that there is no 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 in regulations or a change in the interpretation of regulations gives rise to this.

9.5 If a Party fails to fulfil an agreed obligation, the other Party may give notice of default to the negligent party whereby the negligent Party is granted a reasonable period of time to still fulfil compliance. If fulfilment also fails then, the negligent party is in default. Notice of default is not necessary if compliance with a strict deadline applies, fulfilment is permanently impossible or if it should be inferred from a statement or the attitude of the other party that it will fail to fulfil its obligation.

9.6 The Controller is entitled to, without prejudice to the provisions in the Processing Terms and Conditions and the related main agreement, and without prejudice to the provisions of the law, to suspend the execution of these Processing Terms and Conditions by means of a registered letter or to terminate the agreement, in whole or in part, without judicial intervention and with immediate effect, after the Controller establishes that:

a) the Processor is applying for (temporary) suspension of payments; or
b) the Processor is applying for bankruptcy or is declared bankrupt; or
c) the company of the Processor is dissolved; or
d) the Processor ceases his business; or
e) there is a substantial change in the control over the activities of the company of the Processor in such a way that it cannot reasonably be expected of the Controller that it will maintain the Processing Terms and 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 fulfil the obligations arising from these Processing Terms and Conditions and that attributable shortcoming is not rectified within 30 days after a written notice of default or one of the other situations referred to in Article 9.5 occurs.

9.7 If the Agreement (s) is terminated prematurely, article 9, paragraphs 2 and 3 shall remain in effect.

Article 10 Liability

10.1 The Processor is liable on the basis of the provisions of article 82 of the GDPR, for direct damage resulting from non-fulfilment of these Processing Terms and Conditions, referring to those instances whereby the obligations of the GDPR specifically addressed to the Processor are not being complied with or if the Processor acted outside of the legitimate instructions from the Controller.

10.2 The Processor is only liable for direct damage insofar as this has arisen due to the activity of Processor. The possible liability of PerfectView is limited per event, whereby a coherent series of events counts as one event limited to the amount as paid out by PerfectView's business liability insurer. If the insurer does not pay out for any reason whatsoever, 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 for the Assignment, which was invoiced in the period of 12 months immediately prior to the damage-causing incident.

10.3 Immediate damage is limited to mean the damages as included in the policy sheets of PerfectView's liability insurance policy.

10.4 Liability for trading loss, including damage due to lost profits or unrealized savings, reputational damage or other indirect or consequential damages is excluded. Also excluded is the liability of PerfectView relating to mutilation, destruction or loss of data or documents, for example in case of a security incident and / or data breach, or the prevention or limitation thereof.

10.5 The aforementioned limitations of liability lapse in the case of intent or gross negligence of PerfectView and / or of its managerial subordinates belonging to the board of directors and / or management.

10.6 If the Processor fails to comply with the obligation laid down in Article 6 paragraph 1 of these Processing Terms and Conditions or fails to do so in time and the Supervisory Authority by effect imposes an administrative fine upon the Controller, the Processor will be liable and the Controller will impose a contractual penalty of the same amount upon the Processor. This fine is not susceptible to set-off or suspension and does not affect the rights of the Controller to compliance and compensation.

10.7 If the Processor receives a penalty imposed by the Supervisory Authority or is instructed to compensate for damage to a data subject as a result of acts or omissions by the Controller, the Controller will indemnify the Processor and, on first request, indemnify him for this penalty or damage, including the (legal) costs.

Article 11 Applicable Law

11.1 The Dutch law is exclusively applicable to these Processing Terms and Conditions and to all disputes that arise from or are related thereto.

11.2 All disputes arising from this Processing Agreement will be settled in the same manner as included in the Agreement of which the General Terms and Conditions of PerfectView forms a part.

Appendix 1: Description security measures

In order to elaborate Article 7, paragraph 1

Appendix 2: Description Processor activities

In order to elaborate Article 3, paragraph 1

Appendix 3: Information to evaluate incidents

In order to elaborate Article 6, paragraph 1 and 5

Appendix 4: Sub-processor register

In order to elaborate Article 8, paragraph 5

Appendix 1: Description of security measures

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

Since personal data is processed in PerfectView CRM Online, such 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 makes great efforts throughout the organisation to ensure optimum information security. The certification is assessed annually by an independent accredited body. The hosting partners ClaraNet and Denit, which serve as subprocessors, are also ISO 27001:2013 certified.

The Netherlands

Both PerfectView and all storage sites and partners that jointly provide the CRM Online platform are Dutch, are physically provided from the Netherlands and fully comply with EU data protection legislation.

Reporting

PerfectView shares information about the measures and results of audits and pen tests relating to information security through 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. The same information security requirements are imposed on subprocessors and their staff.

Responsibilities

All employees of PerfectView have signed a declaration of confidentiality with regard to all information that comes to their attention and specifically for the protection of personal data. 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.

Technical measures

Internet connections

The connection between the PerfectView CRM Online environment 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.

Firewall

As a first level of security, Internet traffic to the CRM Online environment is filtered by an L4 firewall. The firewall ensures protection against attacks such as Syn/UDP/ICMP flood protection, IP spoofing, fragmentation attacks etc.

The 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.

Load balancer

In order to ensure the best possible distribution of the traffic flows and consequently the "load" on the servers, the traffic is sent to the web servers via a load balancer. PerfectView uses an F5 BigIP load balancer for this purpose. As soon as a web server is no longer available, the load balancer allows the User to continue the session on one of the other web servers. The load balancer divides the traffic for the application (online.perfectview.nl) over multiple frontend servers and the traffic for the API's (api.perfectview.nl) over multiple backend servers.

DDos Protection

A DDos protection system has been set up to protect against a DDos attack on the IP numbers/websites of PerfectView CRM Online.

For DDos protection, we use Claranet's Web Acceleration & DoS Protection (WADP) service, which has been developed for organisations with business-critical web applications. The service improves the performance, security and availability of web applications if the underlying servers or platform are under high load due to high traffic or attacked by a DDoS attack.

WADP is on the boundary between the Claranet network and the internet and therefore in front of the website, optimising traffic between the web server and visitors. This allows the website to load much faster and reduces the load on servers.

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.

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

Storage

A storage area network (SAN) is used to store data in the data centre. This storage network ensures a very high availability and redundancy of the stored data. For the active data (configurations, databases, etc.) a different SAN environment is used than for the storage of backups and recovery images.

Each organisation has its own physical database within the storage environment, which keeps data from different customers separated at all times.

Virtualisation

All servers use a virtualisation platform. This virtualisation platform is built on the basis of VMWare techniques and supports High Availability.

Servers

The servers use Microsoft products for operating system software as well as application software. The design is based on the best practices/hardening of Microsoft. In addition, this setup has been further optimised with Microsoft Premier Services for the specific use for PerfectView CRM Online.

Updates

The environment is periodically updated with service updates from the suppliers. The updates for the infrastructure, storage systems and virtualisation are carried out by ClaraNet. The Microsoft and CRM Online application systems are kept up to date by PerfectView. In practice, updates are carried out at least once every 2 months, and if there are urgent updates/patches, this can take place within 1 week.

Backups

All data is backed up every night. The backups are placed in a separate backup environment and synchronised to a different physical location. The backups are stored encrypted for a period of 3 months.

Deletion of (personal) data will take place a.s.a.p. at the request of the person responsible 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 incoming and outgoing e-mail is guided by anti-spam/antivirus filters to prevent/stop unwanted messages. PerfectView closely monitors mail traffic. Mail platforms from Flowmailer and Divinet 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 find out if the certificates, chipers and keys that are being used still score an A Grade in the tests of SSLLabs.com to verify that sufficient cryptographic protection is still active.

Penetration test

At least once a year, the CRM Online platform is extensively tested for vulnerabilities. A so-called black and grey penetration test is carried out 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 takes place on the basis of complex passwords and optional 2-factor authentication. Complexity and password change policies 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 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 restricted to customer-appointed support staff and PerfectView system administrators. Employees of PerfectView will never be asked for confidential information such as password information by e-mail or by phone.

Monitoring

The CRM Online platform is continuously monitored in order to be able to conduct maintenance, fault repair, capacity management, etc. adequately and on time.

Logging

Extensive audit logs are created in the application for data changes and system changes by users and administrators. The logs cannot be modified or manipulated by the user and/or administrator.

Appendix 2: Description of the processor activities

With regard to the definitions of the terms used, reference is made to the processing conditions for PerfectView CRM Online.

1. Processing

This processing register includes two processing operations under the contract between the processor and the controller.

1.1. Processing user data

Purpose	User administration for access to the Application Software by employees of the controller
Legal basis	Execution of the agreement
Data subjects	Employees of the controller
Duration	Duration of the agreement

The following Personal Data will be processed under the Agreement:

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

The processor processes personal data for the controller as follows:

- 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 the controller and data subjects about changes and/or incidents in the Application Software as offered by the processor.

The controller determines which Personal Data is processed.

1.2. Offering Application Software

Purpose	Offering Application Software for the purpose of registering the controller’s business-relations data. Offering 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
Data subjects	Relations, employees of the registered relations and employees of the controller
Duration	Duration of the agreement

The Software Application enables the processing of personal data under the agreement. PerfectView assumes the following personal data and has adjusted its security measures accordingly:

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

The processor processes personal data for the controller as follows:

- User data is stored for the purpose of business-relations management by the controller 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 controller, is available during/after updates and can be restored in case of an emergency situation.

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

The controller determines which personal data is processed and whether the security measures offered are adequate for its processing.

Appendix 3: Information to assess incidents

With regard to the definitions of the terms used, reference is made to the processing conditions for PerfectView CRM Online.

Duty to report data leaks 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.

Appendix 4: Sub-processor register

The processor shall use the sub-processors listed in this Appendix in the performance of the contract. The processor shall update this Appendix in accordance with Article 8 of these processing terms and conditions in case of changes to the sub-processors engaged and shall provide this list to the controller without delay.

With regard to the definitions of the terms used, reference is made to the processing conditions for PerfectView CRM Online.

Hosting

Subprocessor	**Claranet Benelux Holdings B.V.**
Location	Science Park Eindhoven 5630 5692 EN Son
Trade Register registration number:	Chamber of Commerce 594 646 74
Description of the activities	Hosting of the website and the CRM Online platform including redundant utilities, infrastructure storage systems and (server) hardware, access security, firewall and anti-DDos protection.
Certifications	https://www.claranet.nl/certificeringen

Subprocessor	**Denit Internet Services B.V.**
Location	Kabelweg 21 1014 BA Amsterdam
Trade Register registration number:	Chamber of Commerce 341 912 83
Description of the activities	Hosting of the website and the CRM Online platform including redundant utilities, infrastructure storage systems and (server) hardware, access security, firewall and anti-DDos protection.

Certifications	https://denit.nl/over-denit/certificeringen/

Subprocessor	**HetWorks B.V.**
Location	Newtonstraat 19-1 3902 HP Veenendaal
Trade Register registration number:	Chamber of Commerce 73 777 153
Description of the activities	Hosting of www.VerlorenOfGevonden.nl including redundant utilities, infrastructure storage systems and (server) hardware, access security, firewall and anti-DDos protection.

Email providers

Subprocessor	**Flowmailer B.V.**
Location	Van Nelleweg 1 3044 BC Rotterdam
Trade Register registration number:	Chamber of Commerce 621 548 85
Description of the activities	Mail-delivery system for sending transactional, service and system messages from the CRM Online platform. Scanning outgoing mail streams for virus and spam content.

Subprocessor	**Divinet.nl B.V.**
Location	Aldenhofstraat 51 6191 GR Beek
Trade Register registration number:	Chamber of Commerce 140 732 49

Description of the activities	Mail-routing system for receiving mail for the CRM Online platform and sending bulk mail messages from the CRM Online platform. Scanning incoming and outgoing mail streams for virus and spam content.