Data Processing Agreement TriFact365

Version 1.0 (May 2018)

TriFact365 processes personal data for and on behalf of the client since the client has a software subscription with TriFact365. TriFact365 and the client are therefore obliged to conclude a Data Processing Agreement in accordance with the General Data Protection Regulation (GDPR). Since TriFact365 provides a standard application with the associated standard service, TriFact365 has included the Data Processing Agreement in the General Terms and Conditions & SLA. TriFact365 is the 'processor' and the client is the 'controller'. TriFact365 and the client commit to comply with the General Data Protection Regulation (GDPR). For the definitions of concepts we refer to the GDPR. TriFact365 will only process the personal data for and on behalf of the client and to implement the agreement.

Processing instructions

TriFact365 is a Dutch company with an international cloud service for customers. Globally, documents are delivered and processed by clients on behalf of clients through the TriFact365 service. The processing consists of making the TriFact365 service available with the data entered and generated by the client. TriFact365 will not add, modify or delete data without the client having given specific instructions to do so. This instruction can be given via a request.

Within the applications that TriFact365 makes available, various types of personal data can be provided and recorded. The client and TriFact365 are aware that the client can enter all these personal data and/or personal data categories to be created and that TriFact365 will process them. The client is responsible for assessing whether the purpose and nature of the processing fits the services of TriFact365.

The client is aware that personal data can be supplied and processed for several categories of data subjects, for example companies, customers, suppliers and customers of customers who can offer various types of documents. The client is responsible for assessing whether the purpose and nature of the processing fits the service provided by TriFact365.

We record the following personal data from our clients:

Subscription details:	• the desired subscription; • user name.	
Contact details:	• gender; • first and last name; • phone number;	• e-mail adress; • contact details of accountant.
Company details:	• company name; • billing address; • zipcode and city;	• e-mail adress; • phone number.
Financial details:	• bank account; • ascription bank account.	

Confidentiality

TriFact365 is aware that the information that the client shares with TriFact365 and stores within TriFact365 has a secret and business-sensitive character. All TriFact365 employees will deal responsibly with the client’s information during their employment and thereafter, as included in their employment contract with a confidentiality clause. TriFact365 has also entered into a similar confidentiality agreement with all flex workers.

TriFact365 collects anonymous data about the use of its products and services. This data supports TriFact365 to understand if, how and how often certain parts of the product are used. The anonymized data will only be used to improve products and services. TriFact365 will never use the collected user statistics for commercial purposes or offer them for sale to third parties.

Employees with access to customer data

TriFact365 system administrators have full access to customer data. Account managers, support staff and other TriFact365 employees have access to only the personal data necessary for the performance of their work.

TriFact365 is entitled to change assigned access or identification codes. The client treats the access and identification codes confidentially and with care and makes them known to authorized staff only in a personalized manner. TriFact365 is not liable for damage or costs resulting from the use or misuse of access or identification codes.

Security

TriFact365 continues to take appropriate technical and organizational measures to protect the personal data of the client against loss or any form of unlawful processing. When taking the security measures, the risks to be mitigated, the state of the technology and the costs of the security measures were taken into account.

The security measures we take have a security level that matches the nature of the personal data and the scope, context, purposes and risks of the processing.

These measures are regarded as an appropriate security level in the sense of the GDPR. More information can be found on the TriFact365 Security and reliability page on our website.

The client is entitled, in consultation with TriFact365 during the term of the agreement, to check compliance with an independent expert, for example by carrying out an audit. The client will reimburse all costs in connection with this inspection.

Liability

TriFact365 is liable for damage in the context of personal data due to acts or omissions of the subprocessor, whereby the liability limitation from the general terms and conditions applies. The applicable limitation of liability does not apply if there is gross negligence or willful misconduct on the part of the subprocessor. TriFact365 is also not liable in the event of force majeure as defined in the general terms and conditions by itself or on the part of the subprocessor.

If the Personal Data Protection Authority will issue a binding instruction to the controller, the client must immediately inform TriFact365 of this binding instruction. TriFact365 will do everything reasonably expect to make compliance possible. If TriFact365 does not do what can be reasonably expected, resulting in a fine, or if the Dutch Data Protection Authority imposes a fine immediately because there is intent or serious culpable negligence on the part of TriFact365, then the applicable liability restriction aforementioned in the general conditions does not apply.

The client indemnifies TriFact365 against claims from persons whose personal data is registered or processed in the context of a personal registration held by the client or for which the client is otherwise responsible under the law, unless the client proves that the facts that are relevant to the claim underlying only TriFact365 must be allocated.

Subprocessors

To be able to offer our worldwide cloud service at the highest level, TriFact365 uses subprocessors who have access to personal data and process these to make the TriFact365 service possible. A list of subprocessors can be found on the TriFact365 website.

The customer hereby authorizes TriFact365 to use services from subprocessors within the European Economic Area as well as subprocessors in countries within the framework of the TriFact365 agreement where the European Commission has determined that these countries offer an adequate level of protection.

If TriFact365 wishes to make use of subprocessor services located in a country that does not offer an adequate level of protection as referred to above, then TriFact365 will enter into an EU model contract for the benefit of the client as an appropriate guarantee with regard to the subprocessor, pursuant to Decision 2010/87 / EU . If the previous guarantee is met, then the client instructs and authorizes TriFact365 to give subprocessing instructions on behalf of the client and to use all rights of the client towards the subprocessors on the basis of the EU model contract.

If the subprocessor fails to fulfill its data protection obligations, TriFact365 remains liable to the customer for the fulfillment of the subprocessor's obligations. However, TriFact365 is not liable for damage and claims arising from instructions from the customer to subprocessors.

TriFact365 will not have new subprocessors process data without informing the client. The client can object to TriFact365 against a new subprocessor. TriFact365 will handle these objections at board level. If TriFact365 wishes to data be processed by the new subprocessor, the client has the option to terminate the agreement.

Privacy rights

TriFact365 has no control over the personal data made available by the client. Without necessity, given the nature of the assignment given by the client, explicit consent of the client or legal obligation, TriFact365 will not provide the data to third parties or process them for other purposes than for the agreed purposes. The client guarantees that the personal data may be processed on the foundation of a basis mentioned in the GDPR.

TriFact365 will, if a request is made on the grounds of legislation and regulations, make all possible information available to the relevant regulator(s).

Data subjects

The client is responsible for the data entered by the data subjects and thereby for informing and assisting the rights of the data subjects. TriFact365 will never respond to requests from those involved and always refer to the responsible party. TriFact365 will, insofar as this is possible within the application, grant its cooperation to the client so that he can fulfill his legal obligations in the event that a data subject exercises its rights under the GDPR or other applicable regulations concerning the processing of personal data.

Data breach notification obligation

The GDPR requires that any data breaches will be reported to the Data Protection Authority by the controller of the data. TriFact365 will therefore not make any reports to the Dutch Data Protection Authority itself. Of course, TriFact365 will inform the client correctly, timely and completely about relevant incidents, so that the client can fulfill his legal obligations as a controller. The Policy Rules on the data breach notification obligation by the Dutch Data Protection Authority provide more information on this.

If the customer makes a (provisional) report to the Dutch Data Protection Authority and/or the person(s) concerned about a data breach at TriFact365, without the client having previously discussed this with TriFact365, then the customer is liable for all damage suffered by TriFact365 and cost. The client is also obliged to withdraw such a report immediately.

Determining data breach

To determine a data breach, TriFact365 uses the GDPR and the Policy Rules for the data breach notification obligation as a guide.

Notification to the client

If it turns out that TriFact365 has a security incident or data breach, TriFact365 will inform the client about this as soon as possible after TriFact365 has become familiar with the data breach. In order to realize this, TriFact365 ensures that all its employees are able to continue to detect a data breach and TriFact365 expects its contractors to enable TriFact365 to meet these requirements. For the sake of clarity: if there is a data breach at a TriFact365 supplier, then TriFact365 will of course also report this. TriFact365 is the point of contact for the client. The client does not have to contact the suppliers of TriFact365.

Informing the client

Initially, TriFact365 will inform the owner of the subscription about a data breach. If this owner is not (anymore) the right one, this can be adjusted via the portal on the 'Users' page.

Providing information

TriFact365 tries to provide the client with all information the client needs to make a possible report to the Dutch Data Protection Authority and/or the person(s) involved.

Term of informing

The GDPR indicates that a data breach must be reported 'without delay'. According to the Dutch Data Protection Authority, this is without undue delay and if possible no later than 72 hours after discovery by the controller. If a security incident occurs, TriFact365 will inform the client as soon as possible, but no later than 48 hours since the discovery by TriFact365. The client will have to make his own assessment of whether the security incident falls under the term 'data breach' and whether a report to the Dutch Data Protection Authority will have to be made. The customer has 72 hours to do so, after the client has been informed of this.

Progress and measures

TriFact365 will keep the client informed about the progress and the measures being taken. TriFact365 makes agreements with the primary contact person of the initial notification. In any case, TriFact365 keeps the client informed in the event of a change in the situation, the publication of further information and the measures that are taken.

TriFact365 registers all security incidents and handles them according to a fixed procedure.

Deleting data

TriFact365 will remove all personal data at the end of the subscription or return it to the client. TriFact365 will also delete all existing backups after 1 year unless TriFact365 is obliged to store such personal data under EU or Member State law. If the client wants to have the data removed earlier, a request can be submitted. TriFact365 is obliged to comply with this request.

Duration of the Data Processing Agreement

The duration is equal to that of the subscription the client has concluded with TriFact365. Unless otherwise provided in this agreement, rights and obligations in the area of termination are the same as the rights and obligations included in the relevant general terms and conditions & SLA.

Heavy interest of the Data Processing Agreement

In the event of any conflict between the content of this Data Processing Agreement and any other agreement between TriFact365 and client, including the terms and conditions & SLA, the provisions of this Data Processing Agreement shall be leading with regard to the data protection obligations of TriFact365 and the client. Even in the event of doubt as to whether conditions in these other agreements relate to the data protection obligations of TriFact365 and the client, this Data Processing Agreement weighs heaviest.

Validity and enforceability of the Data Processing Agreement

Invalidity or unenforceability of any provision in this Data Processing Agreement shall not affect the validity or enforceability of the other provisions of this Data Processing Agreement. This also applies if this Data Processing Agreement contains an omission.

Any dispute between the client and TriFact365 with respect to this Data Processing Agreement will be submitted to the competent court in Utrecht.