General Terms and Conditions, Service Agreement and Data Processing Agreement

Fortes is focused on continuously optimizing their services and the cooperation with their customers. This means that we can enhance our services. We always inform customers about major changes, for example with a special newsletter or a targeted e-mail.

As we provide a standard application (Fortes Change Cloud) and standard services, the data processing agreement is included in these General Terms and Conditions and Service Agreement. The definitions we use for this purpose are in line with the General Data Protection Regulation (GDPR). We only process personal data at the customer's request to execute the agreement.

V3.0
August 2022

Content

About these General Terms and Conditions, Service Agreement and Data Processing Agreement

We understand that, when you do business with Fortes Solutions BV (Fortes), you would like to know what you can expect from us. This is why we have this "General Terms and Conditions, Service Agreement and Data Processing Agreement" document, in which we clearly describe our services, including the processing of personal data. We do this to be as transparent as possible. That is why we do not have separate General Terms and Conditions or a Data Processing Agreement with legal articles and exceptions. All our agreements must be easily understandable. Any contract specific agreements are applicable and leading if there is a conflict with this document. If there are any questions or ambiguities , we would like to hear from you.

Changes

Fortes is focused on continuously optimizing their services and the cooperation with their customers. This means that we can enhance our services. We always inform customers about major changes, for example with a special newsletter or a targeted e-mail.

Software Agreement

The software agreement is for a duration of twelve (12) months unless otherwise agreed in a separate contract agreement. When you enter into this agreement, you receive a license to use the Fortes Change Cloud software application. These services are invoiced annually in advance.

License

The license includes the product options you purchased, such as number of users, edition and environments. You may only use the license for your own organization. Changes in the license can be requested by phone or e-mail (sales@fortes.nl), taking into account a possible notice period.

Service

You are entitled to service (Customer Support and Product Updates) for the duration of the agreement.

Pricing

Fortes is entitled to index the prices annually on the basis of the consumer price index figure (CPI) of the Central Bureau of Statistics (CBS).

Automatic renewal of the contract and termination of the software agreement

After the contract expiry date, the contract is automatically renewed. Typically, the extension is for one year (12 months) or for a different renewal period as agreed in a separate contract. Cancellation by e-mail or registered letter of all agreements must happen at least two (2) months before expiry of the active contract period.

Fortes has the right to terminate the agreement if the customer fails to meet their obligations, has filed for suspension of payment or bankruptcy. The customer may terminate the agreement, if Fortes fails to comply with their obligations under the agreement. Both parties will be given the opportunity to still fulfill their obligations.

How do we handle customer data after the agreement has ended?

Before termination, you can export all data in common formats (such as MS-Excel, CSV and PDF). We keep a backup of all data on the production environment. After 30 days we permanently delete this data.

We can also delete the data earlier on request. Data remains fully available if you continue the subscription with fewer users.

Invoicing

Fortes invoices:
- Licenses: yearly in advance;
- Consultancy: monthly in arrears or in installments as agreed on.

Payment term is 30 days from invoice date.

Liability

Liability

We guarantee that Fortes Change Cloud meets the specifications provided. In case of errors, we will always correct them as soon as possible. Unfortunately, we cannot guarantee that our software will meet the customer goal, unless an explicit agreement is made regarding these goals. If these goals are communicated, we can brainstorm with you. We take great care to ensure the correct operation of Fortes Change Cloud and implementation of our services.

If, despite these efforts, the use of the Fortes Change Cloud results in damages for which we are held liable, our liability is limited to the lesser of the following two amounts:

First amount: € 1,000,000.-- per event or series of events with a common cause whereby the aggregate can never exceed € 2,000,000.-- per calendar year.

Second amount: the total amount invoiced by Fortes to the customer for licenses in the twelve (12) months prior to the event.

We exclude liability for indirect damages (including but not limited to: loss of sales, profits and opportunities).

We cannot apply the liability limitations if there is willful or deliberate reckless conduct of Fortes or our employees. Our liability is excluded if you or third parties engaged by you have made changes to the contracted products; this is explicitly forbidden. Fortes and the customer are not liable to each other in case of force majeure in the sense of the law. Force majeure also includes: force majeure of suppliers of the parties, improper fulfillment of obligations by suppliers prescribed to us by you, disturbances in the power grid and disturbances that affect data traffic insofar as the cause is not attributable to the parties themselves.

Professional and Business Liability Insurance

We have a combined Professional and Business Liability insurance for exceptional calamities that we cannot or do not want to bear ourselves.

If you have a complaint or claim, it is important that you report it to us as soon as possible. We can then start the process of finding a solution.

Moreover, we must also report a claim to our insurer. No matter the issue, we always aim to solve the issue in a mutually agreeable way.

Services

To get the most out of Fortes Change Cloud, it is important to correctly configure it. We support you with consultants while implementing Fortes Change Cloud. To be able to work properly with Fortes Change Cloud, it is necessary that users attend training courses or workshops. We use selected partners to support our customers during implementation and beyond.

Customer Support

Customer support services are described under the Customer Support section.

Account manager

The account manager is your primary contact with Fortes. For questions about your subscription, changes to the software, changes to contact persons and other questions, you can contact your account manager. If you do not know who your account manager is, you can also send an email to sales@fortes.nl.

Implementation and consultancy

We appoint a lead consultant to supervise the implementation phase. Together with you, the lead consultant defines the project plan which outlines the planning, objectives and responsibilities. You will allocate a contact person who is available to work closely with our lead consultant thus ensuring successful implementation of the project. You can schedule incidental or additional consulting work for one (1) or more separate days in consultation with the account manager. A consultancy working day is effectively eight (8) hours, a half day is four (4) hours. The customer is handed over to the Customer Support Center once the implementation phase is completed.

Training

To be able to work properly with Fortes Change Cloud, it is necessary for users to attend training and/or workshops. These are provided by our selected partners.

Application administrator

To ensure that the Fortes software remains correctly configured and managed, it is extremely important that the local (customer location) application administration is well organized. We expect our customers to assign at least one (1) person in the customer organization to perform application administration of the Fortes software.

Customer Support Center

General information regarding support and incidents

Fortes Support Center staff troubleshoot incidents and answer questions regarding Fortes Change Cloud. Any report made to the Support Center is called an “incident”. An incident can be an error, malfunction, request or user question. Registered Fortes Change Cloud users and administrators can open an incident using the Customer Support Portal and directly contact the Support Center.
The conditions for receiving support as described in this Service Agreement are:
- The application must be used in accordance with its intended use;
- You must provide support when required to enable us to resolve the incident;
- You must provide us access to systems when required to enable incident analysis and/or resolve the incident.

Our support and corresponding response times do not include: work carried out at your premises, installation of updates/patches, advice or support for external systems/software, analyzing/resolving problems due to your hardware and/or operating systems (unless caused by direct action of Fortes).

Registration of incidents

Before registering an incident, check the information available on the Customer Support Portal and all other available documentation (online/print). If a solution is not available, you can register an incident for the Support Center online using the Customer Portal. Each incident is assigned a priority by the support employee. This priority determines how quickly the incident is dealt with. In acute situations, the incident must be registered on the Customer Support Portal before you contact the Support Center by phone.
You can follow the progress of the incident on the Customer Support Portal. After each status change, you will receive an update by email. At each stage of the incident, you can add additional information to the ticket.

Priorities and response times

Each incident is assigned a priority by the support person handling the incident. The guidelines for prioritization and associated response times are as follows.

Urgent (Priority 1)

An urgent incident implies that the application cannot be used at all or is functionally disrupted to such an extent that the application cannot be used. Business critical tasks cannot be performed. For these incidents, we will continuously work on realizing a (temporary) solution. The temporary solution will be converted later into a permanent solution, if applicable. You will be informed at least twice a day. First response within 1 hour, a detailed response within 4 working hours.

High (Priority 2)

A high priority incident implies that the functionality of the application is seriously affected but work can continue. Important tasks cannot be performed. For these incidents, we will implement a (temporary) solution as soon as possible. The temporary solution will be converted later into a permanent solution, if applicable. You will be informed at least once a day. First response within 4 working hours, a detailed response within 8 working hours.

Normal (Priority 3)

A normal priority incident affects daily operations, but normal work can continue. Important tasks can be carried out. For these incidents, we will realize a solution in the shortest possible time, taking into account planning and availability. You will be informed at least once a week during analysis of the problem and determination of the solution. First response within 8 working hours, a detailed response within 16 working hours.

Low (Priority 4)

A low priority incident will not affect daily usage. For these incidents, we will in all reasonableness realize a solution, taking into account planning and availability. You will be informed at least once every two weeks during analysis of the problem and determination of the solution. Initial response within 16 working hours, a detailed response within 96 working hours

Note: all incidents for non-production environments are automatically classified one level lower.

Availability of the Customer Support Center

The Customer Support Portal provides up-to-date, relevant information which answers the majority of frequently asked questions and is accessible 24/7. The Support Center is available by phone Monday to

Friday during business hours (09:00 - 17:00 Central European Time), with the exception of Dutch public holidays.

Additional support outside of working hours

Support required during critical events outside the regular Customer Support Center availability, can be requested from the Support Center (for example, for support when upgrading systems that are not hosted by us). This must be requested at least five (5) working days in advance. To do this, contact your account manager. The extra support will be charged at an hourly rate based on hours worked.

Access to customer environment

While handling an incident, a Support Center employee can request access to your environment in several ways:
- By remotely watching with you using screensharing software such as TeamViewer;
- By requesting a backup of your environment for internal analysis;
- You give our Support Center temporary access to your environment whereby you determine the authorization level.

Product

Development and versioning

We ensure that you can work with the latest version of Fortes Change Cloud. Legal changes and necessary updates are only made to the latest version of the software. Each release is provided with release notes describing which parts have been changed. The expected installation of a new version is announced in advance and agreed with you.

Intellectual property rights

We develop and deliver the Fortes Change Cloud software product. The intellectual property rights of Fortes Change Cloud are (and will remain) vested in Fortes. During the term of the agreement, you may only use Fortes Change Cloud for your own organization under the agreed conditions. If a third party claims to hold intellectual property rights to the software, Fortes will indemnify you. A condition for this is that you inform Fortes of this claim as soon as possible, cooperate with the investigation and leave the handling of the case entirely to Fortes. Should the court determine that the intellectual property indeed lies with the third party, Fortes will ensure that you can continue to use the software or provide you with equivalent software.

Local (on-premises) installation

You may choose to install Fortes Change Cloud locally (however, this is not recommended). In such a case, you are responsible for installing and updating Fortes Change Cloud. The time taken to resolve incidents can be longer with local installations. For advice and support of the local infrastructure, you can make use of our services, which will be billed directly on the basis of separate agreements.

System requirements and product support

The system requirements and product support necessary for correct operation of Fortes Change Cloud are described in the documentation on the Customer Service Portal. You must ensure that your own infrastructure is and remains compliant to these requirements.

License

As a user with a local installation, you receive a new license key every twelve (12) months in which the purchased Fortes Change Cloud product components are encrypted with corresponding numbers (e.g. users, edition).

Fortes Change Cloud

Our software products are reliable and secure. We work with external parties to deliver Fortes Change Cloud. The data centers containing our servers are located in the Netherlands and subject to Dutch law and regulations. In addition, they meet the highest standards of physical security.

Availability

The Fortes Change Cloud software product has an availability of 99.9% or better. The availability and performance of Fortes Change Cloud are continuously monitored. In the event of an outage, you will be notified by email and kept up to date on the progress of the outage. In addition to outages, Fortes Change Cloud may also be unavailable in the following situations (not counting towards the 99.9% availability mentioned above):
- Pre-announced preventive maintenance;
- Installation of a new version of Fortes Change Cloud;
- Scheduled maintenance that has been agreed with the customer;
- Calamities resulting from natural disasters and other force majeure situations.

Performance

Fortes Change Cloud should perform within specification. The performance is affected by your internet connection and the configuration of your environment. In the event of performance issues, contact the Support Center.

Local installations are supported on the basis of best effort, but no guarantees can be given for performance, as this also depends on the hardware you have deployed.

Security

We ensure proper deployment of resources, methods and techniques to safeguard the availability, integrity and confidentiality of Fortes Change Cloud. Checking for misuse of the software is part of the (daily) standard monitoring activities. The information security of Fortes Change Cloud is externally audited and certified to ISO 27001. Fortes Change Cloud is hosted in data centers which are also ISO 27001 certified. Additional information on the data centers is available, upon request.

Access security (user authentication)

Each user has a unique username and personal profile. We recommend using Single-Sign-On (SSO) technology for user authentication which is

more secure and convenient for users. We can provide support in coupling the Fortes application to Single-Sign-On (SSO) services. Fortes Change Cloud can also use a username and password, if required.

Continuity

We have disaster recovery procedures in place to prevent loss of data due to system failure, physical destruction or otherwise and to facilitate data recovery. Our servers and infrastructure are fully redundant and distributed across multiple data centers.

Monitoring

We monitor systems, processes and users 24/7 to:
- Pro-actively prevent malfunctions or resolve them at an early stage. Monitoring is aimed at the timely detection of malfunctions and undesirable behavior.
- Collect general user statistics, such as response times. This information is analyzed and if required discussed with you as a possible improvement area.
- Collect anonymous statistics from your environment to improve products and services.

Limited availability due to maintenance

You will be informed preferably seven (7) days and no less than one (1) day in advance if Fortes Change Cloud may be impacted due to maintenance work. These maintenance activities are performed between 20:00 and 07:00 or during weekends. If required, the work will be scheduled in consultation with you. Incidental patches and hotfixes are automatically executed at night without prior notice.

Back-up and restore

The production environment is backed up each night; the development, test or acceptance (DTA) environments are backed up weekly. These back-ups are retained for 30 days and can be restored on request. Additional costs may apply for restoring back-ups.

Development, Test and Acceptance environments (DTA)

In consultation with Fortes, DTA environments can be made available. These environments are mainly used to test new versions of Fortes Change Cloud. A copy of the production environment is placed on the DTA system. A new development, test or acceptance environment (or a refresh) can be requested using the Support Center. The DTA system

and support are not included in the Fortes Change Cloud license, additional costs may apply.

Fair use

We apply a "fair use principle" to the use and deployment of parts of Fortes Change Cloud other than for their intended purpose. We will contact you should you violate the fair use principle and we will try to find a solution together . However, if a solution cannot be found during the consultation with you, we retain the right to terminate your use of Fortes Change Cloud.

Data Processing Agreement Fortes Change Cloud

We process personal data for and on behalf of the customer. The General Data Protection Regulation identifies Fortes as a “data processor” and the customer as a "data controller". Within the meaning of the General Data Protection Regulation (GDPR), Fortes and the customer are required to enter into a data processing agreement. Because Fortes provides a standard application (Fortes Change Cloud) and standard services, the data processing agreement is included in these General Terms and Conditions and Service Agreement. The definitions we use for this purpose are in line with the General Data Protection Regulation. We only process personal data on your behalf to execute the agreement.

Processing instructions

Our processing consists of providing our applications containing your data. We do not add, modify or remove data without prior written instructions from you via a request or using the Customer Support Portal.

Various types of personal data can be recorded in our software,. Furthermore, you can enter additional personal data or categories which will be processed by us. You are responsible for assessing whether the purpose and nature of the processing meet our defined services.

We collect data on the use of our products. This enables us to understand if, how and how often certain parts of the product are used and to improve our products and services. We do not use the data for any other purpose or make it available to third parties without your written consent.

We will provide customer data to third parties if obliged to do so under law. We take various measures to provide maximum protection of your data. Only authorized users have access by applying safeguards.

All customer data is stored separately for each customer. Only our administrators are able to access all customer data. Our servers are located in data centers in The Netherlands and meet the highest standards of physical security.

Confidentiality

We are aware that the information you share with us and store in Fortes Change Cloud is confidential and business-sensitive. Our employees, as

required by the confidentiality clause in their employment contract , handle your data responsibly.

Privacy rights

As defined by the GDPR, you are the data controller and as such we have no control over any personal data you make available. We do not, without your explicit consent or legal obligation, make the data available to third parties. We do not process your data for any purpose other than those agreed on.

You guarantee that the personal data may be processed in accordance with the GDPR. As required by any applicable laws and regulations, your auditors (internal or external) or those hired by the supervisory body can conduct audits to verify our compliance with the terms and conditions set out in the agreement, any supervisory regulations and/or any applicable laws. We will inform you of any audit as soon as possible, provided this is not prohibited.

Involved parties

You are responsible for the entered data of the data subjects. In addition, you are responsible for informing them of their rights and assisting them. We never respond to requests from the data subjects and always refer them to the responsible party. If the data subject exercises their rights under the GDPR or any other applicable regulations for processing of personal data, we will always endeavor to assist you, within the boundaries of what is possible within the application, enabling you to comply with any legal obligations.

Security

We are ISO 27001 certified which means that we do everything within our power to secure your personal data against loss or other unlawful processing. ISO 27001 in combination with our own security measures provide the required GDPR security level. We will always help you to meet your obligations regarding the GDPR and similar laws and regulations for the processing of personal data. In consultation, you can have an audit performed during the term of the agreement. This is at your own expense.

We are liable for any damages with respect to personal data caused by acts or omissions of Fortes or their sub-processor. The limitation of liability described in the Liability section applies here. We cannot invoke a limitation of liability for a remedy under the GDPR, article 82.

If your local Data Protection Authority (in the Netherlands Autoriteit Persoonsgegevens) gives you a binding instruction, you must report this

to us immediately. We will do everything possible to ensure compliance. If we fail to do so and this results in a fine, or if the local Data Protection Authority (DPA) imposes a fine immediately, due to intentional or gross culpable negligence on our part, the liability limitation in the Liability section is not applicable.

Sub-processors

We process your data in data centers of our sub-processor, Equinix B.V. (CoC: 24429748). Their data centers are located exclusively in the Netherlands and are subject to Dutch law and regulations. They comply with strict Dutch and European legislation for access security and continuity. The data centers are at least ISO 27001 certified. The data is processed by us and our sub-processor only within the European Economic Area. The same obligations apply to us and our sub-processor(s).

The optional Premium Edition of Fortes Change Cloud includes PowerBI Embedded , a Microsoft Azure service, which is used to deliver management dashboards. This makes Microsoft Ireland Operations Ltd (CoC: IE8256796) also a sub-processor. These management dashboards are delivered from Microsoft data centers in Western Europe.

We do not allow new sub-processors to process data without informing you in a timely manner (at least 4 weeks in advance). You can object to a sub-processor at any time. We discuss such objections at senior management level. If we allow the new sub-processor to process data, you are within your rights to terminate the contract with immediate effect.

Mandatory notification for data breaches

In the event we have a data breach (as referred to in GDPR, article 33) that must be reported by you to the local DPA and the affected data subject(s), we will inform you as soon as the data breach has been identified. We aim to provide you with all the information required to make a complete report to the local DPA and/or the data subject(s). If this information is not available (e.g. because the data breach is under investigation by Fortes), we will provide you with sufficient information to enable you to make a preliminary notification to the local DPA and/or the data subject(s).

When the customer notifies the local DPA and/or the data subject(s) with respect to a data breach at Fortes, while it is apparently clear to the customer that this is not the case as referred to in GDPR, article 33, the customer shall be liable for all damages and costs (including

damage to our reputation). The customer is also obliged to immediately withdraw such a notification.

If you notify the local DPA and/or the data subject(s) about a data breach at Fortes, we request you inform us before you inform the local DPA. We can then together take the correct follow-up actions.

Determination of a data breach

We use the GDPR and the Data Breach Notification Policy to determine a personal data breach.

Customer notification

When we have a security incident or data breach, we will inform you as soon as possible. All our employees can report a data breach using our standard operating procedure (workflow). In addition, we expect contractors to follow this procedure. Should a data breach occur at a sub-processor, the same notification policy applies, with the exception that we are your point of contact.

Notification term

Under the GDPR, security breaches must be reported "without delay". According to the local DPA, this is without undue delay and, if possible, no later than 72 hours after discovery by the responsible party. In the event of a security incident, we will inform you no later than 48 hours after the discovery. You must assess for yourself if the security incident qualifies as a "data leak" and whether notification to the local DPA is mandatory. After you have been informed by us, you must do this within 72 hours.

Providing information

We always aim to supply all relevant information immediately to enable you to notify the local DPA and/or the data subject(s) concerned.

Progress and measures

We will inform you of the status and our measures. We will make agreements about this with the primary contact person indicated in the report. We will keep you informed if the situation changes, when there is additional information and about the measures we are taking. We register all security incidents and handle them in accordance with our standard operating procedure (workflow). As part of our yearly ISO

27001 certification audit, the security incident registration and handling procedures are reviewed.

Data deletion

On termination of the agreement, we delete all your data, as described in 'How do we handle customer data after the agreement has ended?'. At your request, we are obliged to remove your data at any time.

Legal Affairs

Applicable law and disputes

The customer and Fortes agree that Dutch law is applicable to all agreements and disputes. For this reason, the Vienna Sales Convention which has its own rules for international purchase agreements, is excluded. Any disputes between the customer and Fortes will be exclusively brought before the District Court Midden-Nederland, location Utrecht, The Netherlands.

Disclaimer

Fortes reserves the right to change the Service Agreement, General Terms and Conditions and the Data Processing Agreement.

Any changes will be published on the Customer Support Portal. In the case of major changes, you will be notified by email.