

General Terms and Conditions, Service Agreement and Data Processing Agreement

The Supplier aims to continuously optimise its services and its cooperation with its Clients. This may mean that the Supplier makes changes to its services. The Supplier always notifies its Clients of major changes, for example by newsletter or a dedicated e-mail.

Because the Supplier provides a standard application (Fortes Change Cloud) and standard services, the data processing agreement has been incorporated into these General Terms and Conditions and Service Agreement. The definitions used are aligned with the GDPR. The Supplier processes personal data solely on the instructions of the Client and in order to perform the agreement.

V4.0

August 2026

Table of contents

About these General Terms and Conditions, Service Agreement and Data Processing Agreement	4
Parties	4
Purpose and background	4
Related documents	5
Changes	5
1 General Terms and Conditions	6
1.1 Agreement	6
1.1.1 Service	6
1.1.2 Right of use	6
1.1.3 Term of the agreement	6
1.1.4 Indexation	6
1.1.5 Termination of the agreement	6
1.2 Liability	7
1.2.1 Limitation of liability	7
1.2.2 Professional and General Liability Insurance	8
1.3 Legal Matters	9
1.3.1 Governing law and disputes	9
1.3.2 Changes to these terms and conditions	9
2 Service Agreement (SLA)	10
2.1 Term and duration of the SLA	10
2.2 Services	10
2.2.1 Customer Support	10
2.2.2 Account manager	10
2.2.3 Implementation and consultancy	11
2.2.4 Training	11
2.2.5 Functional management	11
2.3 Customer Support Center	11
2.3.1 Ticket types and definitions	11
2.3.2 General information regarding support and incidents	12
2.3.3 Registration of tickets	12
2.3.4 Priorities and response times	13
2.3.5 Requests for Change (RFC)	14
2.3.6 Availability of the Customer Support Center	15
2.3.7 Additional support outside working hours	15
2.3.8 Access to the customer environment	15
2.4 Product	16
2.4.1 Development and version management	16
2.4.2 Ownership rights	17
2.4.3 Local installation	17

2.5	Fortes Change Cloud	18
2.5.1	Availability	18
2.5.2	Performance	18
2.5.3	Security	18
2.5.4	Access	19
2.5.5	Continuity	19
2.5.6	Monitoring	19
2.5.7	Unavailability due to maintenance	19
2.5.8	Back-up & restore	20
2.5.9	Test and acceptance environments	20
2.5.10	Fair use	20
2.5.11	Documentation	20
2.6	Escalation and communication	21
2.6.1	Roles and escalation line at the Client	21
2.6.2	Escalation procedure	21
2.6.3	Reporting of escalations	22
2.6.4	Evaluation of escalations	22
3	Data Processing Agreement	23
3.1	Data Processing Agreement Fortes Change Cloud	23
3.1.1	Processing instructions	23
3.1.2	Duty of confidentiality	24
3.1.3	Privacy rights	24
3.1.4	Data subjects	24
3.1.5	Security	25
3.1.6	Sub-processors	25
3.1.7	Obligation to report data breaches	26
3.1.8	Deleting data	27

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

When the Client does business with the Supplier (Fortes Solutions B.V.), the Client wants to know what it can expect from the Supplier. That is why the Supplier has drawn up these “General Terms and Conditions, Service Agreement and Data Processing Agreement”, which clearly describe the services, including the processing of personal data. The Supplier strives for maximum transparency and therefore does not maintain separate General Terms and Conditions or a separate Data Processing Agreement with stand-alone legal articles and exceptions; the agreements should be easy for everyone to understand. Individual arrangements set out in the contract also apply and prevail to the extent they conflict with this document. If anything is unclear, the Supplier would be glad to hear about it.

Parties

The following parties are involved in these General Terms and Conditions, Service Agreement and Data Processing Agreement:

- Supplier: Fortes Solutions B.V., established at Capitooll 15 in Enschede, hereinafter referred to as the “Supplier” (also referred to as “Fortes”).
- Client: the legal entity or organisation that has entered into an agreement with the Supplier as stated in the contract, hereinafter referred to as the “Client”.

Wherever this document refers to the “Supplier” or the “Client”, the party described above is meant.

Purpose and background

This document describes the tasks and responsibilities of the Supplier and the Client in relation to the services purchased. The qualitative and quantitative arrangements for the intended level of service are described in the form of service levels.

The objective is to provide a clear description of the mutual expectations regarding the products and/or services delivered by the Supplier. The Supplier and the Client aim to achieve the service levels through effective cooperation. The response times, answer times and

target resolution times referred to in this document are obligations to use best efforts and do not constitute strict deadlines; only periods expressly designated as strict deadlines in the main agreement qualify as such.

Related documents

This document forms part of the agreement(s) concluded between the Client and the Supplier. In the event of any conflict between this document and the contract, the individual arrangements in the contract prevail.

Changes

The Supplier aims to continuously optimise its services and its cooperation with its Clients. This may mean that the Supplier makes changes to its services. The Supplier always notifies its Clients of major changes, for example by newsletter or a dedicated e-mail.

1 General Terms and Conditions

This part describes the contractual arrangements between the Client and the Supplier: the agreement, the licence, the term, termination, liability and the legal provisions.

1.1 Agreement

The agreement between the Client and the Supplier is entered into for an indefinite period, unless otherwise agreed in the contract. Upon entering into this agreement, the Client receives a licence to use Fortes Change Cloud. The Client is invoiced annually for this licence.

1.1.1 Service

For the duration of the agreement, the Client is entitled to service (Customer Support and product updates).

1.1.2 Right of use

The licence for Fortes Change Cloud may only be used:

- during the term of the contract;
- for the Client's own business;
- for the maximum quantities stated in the contract.

1.1.3 Term of the agreement

The agreements to which these terms and conditions apply are entered into for an indefinite period with a minimum term of one year, unless otherwise agreed.

1.1.4 Indexation

The Supplier reserves the right to index its rates annually in line with the consumer price index (CPI) published by Statistics Netherlands (CBS).

1.1.5 Termination of the agreement

Either party may terminate the agreement by giving notice. The notice period for the Client is two months before the end date of the current agreement. The Supplier is entitled to terminate the agreement if the Client fails to fulfil its obligations or has applied for suspension of payments or bankruptcy. The Client may likewise terminate the agreement if the Supplier fails to fulfil its obligations under the

agreement. Both parties will be given the opportunity to still fulfil their obligations.

How do we handle customer data after termination of the agreement?

Before termination, the Client can export all data in common formats (such as MS Excel, CSV and PDF). The Supplier retains a back-up of all data on the production environment. After 30 days, the Supplier permanently deletes this data. On request, the Supplier can also delete the data sooner. The data remains fully available if the Client continues the subscription with fewer users.

Exit arrangement (steps upon termination)

To ensure a smooth transition, the Supplier and the Client follow the steps below upon termination:

- Export by the Client: during the term and up to the end date, the Client can export all data itself in common formats (MS Excel, CSV and PDF).
- Support with export or migration: on request, the Supplier provides additional support. These additional activities are charged on a time-and-materials basis.
- Retention period: after the end date, the Supplier retains the back-up of the production environment for a further 30 days. At the Client's request, the Supplier can delete the data sooner.
- Permanent deletion and confirmation: after 30 days (or sooner on request), the Supplier permanently deletes the data. On request, the Supplier provides written confirmation of the deletion.
- Continuation with fewer users: if the Client chooses to continue the subscription with fewer users, the data remains fully available.

1.2 Liability

1.2.1 Limitation of liability

The Supplier warrants that Fortes Change Cloud complies with the specifications it publishes. In the event of defects, the Supplier will always remedy these as quickly as possible. Unless expressly agreed otherwise, the Supplier cannot warrant that its software will meet all the purposes the Client may have. If those purposes are made known, the Supplier will of course be happy to give its input. The Supplier takes

great care to ensure the proper functioning of Fortes Change Cloud and the correct performance of its services.

If, despite these efforts, the use of Fortes Change Cloud results in damage for which the Supplier is held liable, the Supplier's liability is limited to the lower of the following two amounts:

First amount: EUR 100,000 per event or series of events with a common cause, whereby the aggregate amount can never exceed EUR 250,000 per calendar year.

Second amount: the total amount the Supplier has charged the Client for Licences in the twelve months preceding the event.

The Supplier excludes its liability for indirect damage (including, but not limited to: lost turnover, lost profit and missed opportunities).

The Supplier cannot invoke the limitations of liability in the event of intentional or wilfully reckless conduct by the Supplier itself or by its employees. The Supplier's liability is excluded if the Client or third parties engaged by the Client have made changes to the Supplier's products, which is not permitted. The Supplier and the Client are not liable towards each other in the event of force majeure within the meaning of the law. Force majeure also includes: force majeure affecting the parties' own suppliers, improper performance of obligations by suppliers prescribed to the Supplier by the Client, disruptions in the electricity grid and disruptions that impede data traffic, in so far as the cause thereof is not attributable to the parties themselves.

1.2.2 Professional and General Liability Insurance

The Supplier holds combined Professional and General Liability Insurance for exceptional incidents that the Supplier cannot or does not wish to bear itself.

If the Client has a complaint or claim, it is important that the Client reports this to the Supplier as soon as possible. The Supplier can then start working on a solution straight away. In addition, the Supplier must also report a claim to its insurer. Whatever goes wrong, the Supplier will always seek the right solution in good consultation.

1.3 Legal Matters

1.3.1 Governing law and disputes

The Client and the Supplier choose Dutch law to govern all agreements and disputes. For that reason, the Vienna Sales Convention, which contains its own rules for international sales contracts, is excluded. Any disputes arising between the Client and the Supplier will be submitted exclusively to the Central Netherlands District Court, Utrecht location.

1.3.2 Changes to these terms and conditions

The Supplier reserves the right to amend the SLA, the General Terms and Conditions and the Data Processing Agreement. Changes will be published on the Customer Support Portal and, in the case of major changes, Clients will be notified by e-mail.

2 Service Agreement (SLA)

This part describes the services and the service levels: support, incident handling, response and target values, availability, maintenance, version management and escalation.

2.1 Term and duration of the SLA

The service agreement (SLA) is inextricably linked to the agreement. The term of the SLA runs concurrently with the term of the agreement.

2.2 Services

To get the most out of Fortes Change Cloud, it is important to configure it properly from the outset. The Supplier supports the Client with consultants in implementing Fortes Change Cloud. In order to work effectively with Fortes Change Cloud, it is essential that users attend training. The Supplier works with selected partners.

2.2.1 Customer Support

The services relating to Customer Support are described in the chapter Customer Support Center.

2.2.2 Account manager

For the Client, the account manager is the primary point of contact within the Supplier's organisation. For questions about the subscription, modifications to the software, changes of contact persons and any other questions, the Client can always turn to the account manager. If the Client does not know who the account manager is, the Client can send an e-mail to sales@fortes.nl.

Keeping contact persons up to date. The Client enters the contact persons itself and keeps them up to date in Fortes Change Cloud. This concerns at least the roles of functional management, administration/finance and security/privacy. The Supplier uses these details for important communications, such as announcements of maintenance and releases, status updates on tickets and notifications in the event of an (imminent) data breach. The Supplier is entitled to rely on the contact persons as registered in the software; the Client processes any changes itself as soon as possible or passes them on to the account manager.

2.2.3 Implementation and consultancy

The Supplier appoints a lead consultant to guide the implementation process. Together with the Client, the lead consultant draws up a project plan setting out the schedule, objectives and responsibilities. The Client ensures that a contact person is available to work together on the success of the process. Incidental or additional consultancy work of one (1) or more separate days can be scheduled by the Client in consultation with the Supplier's account manager. A consultancy working day amounts to 8 effective hours; a half day to 4 hours. The Client hands consultancy over to the Support Center as soon as the implementation project has been completed.

2.2.4 Training

In order to work effectively with Fortes Change Cloud, it is essential that users attend training. The Supplier provides its Clients with up-to-date material via the knowledge portal and with training facilitated by the Supplier's partners.

2.2.5 Functional management

To ensure that the software remains properly configured and managed on an ongoing basis, it is very important that functional management is properly assigned and organised within the Client's organisation. The Supplier expects its Clients to designate at least one (1) person within their organisation to perform functional management of the Supplier's software.

2.3 Customer Support Center

The Supplier has its own support organisation. The staff of the Supplier's Support Center resolve problems and answer questions about Fortes Change Cloud. Tickets can be registered via the Customer Support Portal. The Supplier expects the Client always to consult the information on the Customer Support Portal first before registering a ticket. Every ticket is assessed and classified; if it concerns an incident (disruption), it is assigned a priority. The Client can follow the handling of the ticket via the Customer Support Portal.

2.3.1 Ticket types and definitions

After registration, a ticket submitted to the Support Center is classified as one of the following types:

- Incident: an unplanned interruption or reduction in the quality of the service (disruption). See 'Priorities and response times' and 'Target resolution times and workarounds'.
- Question (user question): a functional question about the service. See 'Questions (user questions)'.
- Change (Request for Change, RFC): a request to implement a change to the service. See 'Requests for Change (RFC)'.

2.3.2 General information regarding support and incidents

The staff of the Supplier's Support Center resolve problems and answer questions about Fortes Change Cloud. The various ticket types are described under 'Ticket types and definitions'. Registered users and administrators of Fortes Change Cloud can register a ticket via the Customer Support Portal and contact the Support Center for assistance.

The conditions for receiving support as described in this SLA are:

- the Client must use the application in accordance with its intended use;
- the Client must provide reasonable assistance to the Supplier in resolving the incident;
- the Client must give the Supplier access to systems where necessary in order to analyse and/or resolve the problem.

The Supplier's support and the associated response times do not cover: work at the Client's premises, installation of updates/patches, advice or support for external systems/software, or the analysis/resolution of problems resulting from the Client's hardware and/or operating systems (unless caused directly by the Supplier).

2.3.3 Registration of tickets

The Supplier expects the Client always to consult the Customer Support Portal and all other available documentation (online/printed) first. If no solution is available, the Client can register a ticket online with the Support Center via the Customer Support Portal. Every ticket is assessed and classified by the support employee and, if it concerns an incident, assigned a priority that determines how it is handled. In an acute situation, the Client may contact the Support Center by

telephone after registering; in all cases the ticket must be recorded in detail via the Customer Support Portal.

The Client can follow the handling of the ticket via the Customer Support Portal. It receives an update by e-mail on every change of status. The Client is involved in the handling and can add responses and additional information.

2.3.4 Priorities and response times

Every incident is assigned a priority. This is assigned by the support employee who takes up the incident. The guidelines for prioritisation and the associated response times are as follows.

Urgent (Prio 1). An urgent incident means that the application cannot be used at all or is functionally disrupted to such an extent that it cannot be used. Business-critical tasks cannot be performed. For these incidents, the Supplier will work continuously on achieving a (temporary) solution. A temporary solution will later be converted into a permanent solution, where applicable. The Client is kept informed at least twice a day. First response within 1 working hour, substantive response within 4 working hours.

High (Prio 2). A high-priority incident means that the functionality of the application is seriously affected but work can continue. Important tasks cannot be performed. For these incidents, the Supplier will achieve a (temporary) solution as soon as possible. A temporary solution will later be converted into a permanent solution, where applicable. The Client is kept informed at least once a day. First response within 4 working hours, substantive response within 8 working hours.

Normal (Prio 3). A normal-priority incident affects day-to-day use, but normal work can continue. Important tasks can be performed. For these incidents, the Supplier will achieve a solution at the earliest possible opportunity, taking account of planning and availability. The Client is kept informed at least once a week while the problem is being analysed and the solution determined. First response within 8 working hours, substantive response within 16 working hours.

Low (Prio 4). A low-priority incident has no effect on day-to-day use. For these incidents, the Supplier will achieve a solution on a reasonable-efforts basis, taking account of planning and availability. The Client is kept informed at least once every two weeks while the problem is being analysed and the solution determined. First response within 16 working

hours, substantive response within 96 working hours. Tickets for non-production environments (test and acceptance) are handled one priority level lower, with prio 4 as the lowest classification.

Target resolution times and workarounds

In addition to the response times, the Supplier applies target values for making a workaround available. These target values are obligations to use best efforts and not strict deadlines, and apply to providing a workaround, not to a permanent fix. A workaround is a temporary solution that enables the Client to continue working; a structural fix is generally delivered through the regular release cycle (see 'Release cycle: major, minor and patch') and is therefore not tied to a fixed period.

- Prio 1 (urgent): workaround; target value available within 1 working day.
- Prio 2 (high): workaround; target value available within 5 working days.
- Prio 3 (normal) and Prio 4 (low): no fixed workaround period; the solution is included in the planning and the regular release cycle.

Questions (user questions)

Not every ticket is a disruption. A user question (for example "how does function X work?") is registered as a separate ticket type and has its own answer period, independent of the priorities for disruptions:

- First response: within 8 working hours of registration via the Customer Support Portal.
- Substantive answer: within 3 working days. If a question requires more investigation, the Client will receive feedback within this period about the expected handling time.

2.3.5 Requests for Change (RFC)

An improvement proposal or change request is registered as a Request for Change (RFC). A separate handling procedure applies to an RFC:

- The RFC is registered via the Customer Support Portal and is assigned a unique ticket number so that it can be traced.
- The RFC is assessed and, if it fits within the product strategy, placed on the product backlog. Placement on the backlog is not a commitment as to realisation or timing.

- The prioritisation and any realisation of RFCs are determined through the Supplier's regular product management and roadmap process.
- Once an RFC has been placed on the backlog, the associated support ticket is closed. Further progress is tracked via the product roadmap and the release notes, and no longer as an open incident.

2.3.6 Availability of the Customer Support Center

Up-to-date and relevant information, providing answers to the majority of questions asked, can be consulted 24x7 via the Customer Support Portal. The Support Center can be reached by telephone from Monday to Friday between 09:00 and 17:00 (Dutch time) on 088 888 4222, with the exception of Dutch public holidays. Tickets are registered via the Customer Support Portal; in addition, the Supplier can be reached by e-mail at support@fortes.nl. Outside office hours (5pm to 9am, Dutch time), the incident number 088 888 4200 is available for Prio 1 incidents.

2.3.7 Additional support outside working hours

For support during critical moments outside the regular availability of the Customer Support Center, the Client can obtain additional support from the Support Center (for example when upgrading systems that are not hosted by the Supplier). This must be requested at least 5 working days in advance via the account manager. This additional support is charged on a time-and-materials basis.

For acute situations outside regular opening hours, the Supplier can be reached by telephone on the incident number 088 888 4200. This number is intended exclusively for Prio 1 incidents (the application is completely unusable or unreachable). Regular questions, requests and Prio 2 to Prio 4 incidents are registered and handled via the Customer Support Portal. Even in the case of a telephone report, the Client registers the incident - where possible beforehand - in the Customer Support Portal, so that the ticket is complete and traceable.

2.3.8 Access to the customer environment

While handling an incident, a member of the Supplier's staff may request access to the customer environment in various ways:

- By viewing the Client's screen remotely together with the Client.

- The support employee requests a back-up of the customer environment for internal investigation. This only takes place at the Client's request or with the Client's consent and in accordance with the Data Processing Agreement (part 3).
- The Client grants the Supplier's employee temporary access to the customer environment. The Client can determine the authorisation level itself.

2.4 Product

2.4.1 Development and version management

The Supplier ensures that the Client can work with the most recent version of Fortes Change Cloud. Statutory changes and necessary updates are only implemented in the latest version of the software. Every delivery is accompanied by release notes. These describe which components have been modified. The expected installation of a new version is announced in advance and coordinated with the Client.

Release cycle: major, minor and patch

The Supplier applies semantic versioning based on the major.minor.patch principle and has the following release cycle:

- Major release (for example from 5.x.x to 6.0.0): substantial functional extensions and/or technical changes that may impact configuration or use. The Supplier applies a six-monthly major release cycle; major releases are announced well in advance and coordinated with the Client.
- Minor release (for example from 6.1.x to 6.2.0): new, backwards-compatible functionality and improvements, delivered in an interim minor release cycle. Minor releases are announced via the release notes.
- Patch release (for example from 6.2.0 to 6.2.1): bug fixes and security updates in a continuous patch release cycle. Patches and hotfixes may be delivered on an ongoing basis and, where necessary, without prior notice (see 'Unavailability due to maintenance').

All Clients are updated to the latest version every six months. If desired, a minor release can be installed in the interim where certain functionality is needed ahead of the major release. If a test/acceptance environment is available (not every Client has one), new versions (major

and minor) and any database conversions are first installed on the acceptance environment and only installed on the production environment after approval by the Client's (functional) application management. Always in consultation.

2.4.2 Ownership rights

The Supplier develops and delivers the software product Fortes Change Cloud. The intellectual property rights in Fortes Change Cloud vest (and continue to vest) in the Supplier. During the term of the agreement, the Client may only use Fortes Change Cloud for its own organisation under the agreed conditions. If a third party claims that the intellectual property rights in the software belong to it, the Supplier will indemnify the Client. A condition for this is that the Client informs the Supplier as soon as possible, cooperates with the investigation and leaves the further handling of the matter entirely to the Supplier. If a court establishes that the intellectual property does indeed belong to a third party, the Supplier will ensure that the Client can continue to use the software or will provide the Client with equivalent software.

2.4.3 Local installation

The Client may choose to install Fortes Change Cloud locally (this is not recommended). In that case, the Client is itself responsible for installing and updating Fortes Change Cloud. Resolving incidents may take longer in the case of local installations. For advice and support relating to the local infrastructure, the Client can make use of the Supplier's services, which are charged directly on the basis of separate arrangements.

System requirements and product support. The system requirements and product support necessary for the proper functioning of Fortes Change Cloud are described in the documentation available on the Customer Service Portal. The Client ensures that its own infrastructure complies with these requirements as a minimum.

Licence. The Supplier works with an annual licence code in which the purchased product components of Fortes Change Cloud and the associated quantities (including users and modules) are encrypted. The licence code has a term of one (1) year. It is automatically extended by one (1) year once all financial obligations have been met. Changes to the licence can be requested by telephone or by e-mail (sales@fortes.nl).

2.5 Fortes Change Cloud

The Supplier's software products are reliable and secure. The Supplier works with external parties to make Fortes Change Cloud available. The data centres housing the Supplier's servers are located exclusively within the EEA, are subject to Dutch and European laws and regulations and meet the strictest physical security requirements.

2.5.1 Availability

The software product Fortes Change Cloud has an availability of 99.9% per year (measured per calendar year) or better. The availability and performance of Fortes Change Cloud are continuously monitored. In the event of a disruption, the Client is informed by e-mail and kept up to date on developments. In addition to unavailability due to disruptions, Fortes Change Cloud may be unavailable in the following situations, which do not count towards the 99.9% annual availability:

- pre-announced preventive maintenance;
- installation of a new version of Fortes Change Cloud;
- planned maintenance agreed with the Client;
- incidents resulting from natural disasters and other force majeure situations;
- unavailability of embedded Power BI functionality (if used), in so far as caused by the Microsoft service.

2.5.2 Performance

Fortes Change Cloud should perform well. Actual performance also depends on the internet connection and the configuration of the Client's environment. In the event of performance issues, the Support Center can be contacted. Local installations are supported on a best-efforts basis, without any performance guarantees being given, since performance also depends on the Client's hardware.

2.5.3 Security

The Supplier ensures the appropriate deployment of resources, methods and techniques to safeguard the availability, integrity and confidentiality of Fortes Change Cloud. Monitoring for misuse forms part of the (daily) standard monitoring activities. The entire information security system has been audited by an external auditor and is ISO

27001 certified. The data centres where Fortes Change Cloud is hosted are also ISO 27001 certified. Further information about the data centres can be made available on request.

2.5.4 Access

Every user has a personal profile linked to a unique user name with an associated password. If the Client additionally opts for access via another connection, for example via SAML for Single Sign-On (SSO), authentication is NO longer arranged by the Supplier. Access then falls under the Client's policy and responsibility.

2.5.5 Continuity

The Supplier has contingency procedures in place to prevent loss of data through system failure, physical destruction or otherwise, and to facilitate data recovery. The Supplier's servers and infrastructure are fully redundant and distributed across multiple data centres.

2.5.6 Monitoring

The Supplier monitors systems, processes and users 24/7 for the following purposes:

- to prevent disruptions or resolve them at an early stage. Monitoring is aimed at detecting disruptions and undesirable behaviour in good time.
- to collect general user statistics, such as response times. This information is analysed and may be discussed with the Client with a view to improvement.
- to collect anonymous statistics from the customer environment in order to improve products and services.

2.5.7 Unavailability due to maintenance

The Supplier carries out maintenance as far as possible within fixed, periodic maintenance windows. These windows fall outside office hours: between 5pm and 9am (Dutch time) or at weekends. The Supplier informs the Client of planned maintenance that (may) render Fortes Change Cloud unavailable preferably seven (7) days in advance and no later than one (1) day in advance, via the Customer Support Portal and the registered contact persons. Maintenance that may impact use is scheduled in consultation with the Client where necessary. Incidental

patches and hotfixes may, where necessary for continuity or security, be carried out automatically and without prior notice at night.

2.5.8 Back-up & restore

A back-up of the production environment is made every night, with a retention period of 30 days. A back-up of the test and acceptance environment is also made every night, with a retention period of 7 days. Back-ups can be restored on request; charges may apply.

2.5.9 Test and acceptance environments

If agreed, the Supplier can make a test and/or acceptance environment available; not every Client has one. This environment is used to test a new version of Fortes Change Cloud and to test the Client's further developments, such as new processes, working methods and configurations. A copy of the production environment is placed on the acceptance environment. A new or refreshed test/acceptance environment (refresh) can be requested via the Support Center. The test and acceptance environment and the support thereof are not included in the licence as standard; additional costs may apply.

2.5.10 Fair use

The Supplier applies a "fair use principle". This is applied to the use and deployment of components of Fortes Change Cloud other than for their intended purpose. The Supplier will contact the Client if the fair use principle is breached and will seek a solution in consultation with the Client. Only if no solution can be found in consultation with the Client is the Supplier entitled to discontinue the use of Fortes Change Cloud.

2.5.11 Documentation

During the term of the agreement, the Supplier makes Dutch-language documentation available to the Client. This documentation describes the current characteristics and possible uses of the service and is complete, accurate and up to date. The documentation is such that administrators can carry out or modify the configuration, and each page identifies the version of the documentation and of the service to which it relates. The Client may reproduce the documentation free of charge for use within its own organisation, provided that the copyright notices are retained.

2.6 Escalation and communication

2.6.1 Roles and escalation line at the Client

The Client designates the persons who fulfil the roles below and keeps these up to date in the Customer Support Portal (see 'Keeping contact persons up to date'). The names of the roles may differ from one organisation to another; what matters is who actually fulfils the role. The internal line at the Client is as follows:

- User/reporter: reports a disruption or question to the Client's own functional management.
- Functional administrator (application management): first point of contact towards the Supplier, authorised to submit tickets and to discuss the assigned priority.
- Escalation officer/coordinator: engages with the Supplier's account manager if no agreement is reached.
- Ultimate responsible officer: the operations manager is involved in escalation at tactical or strategic level.

2.6.2 Escalation procedure

The Client and the Supplier jointly determine the priority of a ticket. If no agreement is reached at the relevant level on the priority or the actions to be taken, the escalation procedure comes into effect. In the meantime, the ticket continues to be handled in accordance with the applicable priority rules; the escalation procedure runs in parallel. If the Client anticipates a high or urgent priority, telephone contact is required in addition to the ticket submitted via the portal or by e-mail, so that the Supplier can take immediate action.

The escalation steps are:

- Step 1: the Client's functional management contacts the Supplier's Support Center.
- Step 2: if no agreement is reached, the Client's escalation officer engages with the Supplier's account manager.
- Step 3: if no agreement is reached at tactical level, contact takes place (by telephone and/or in person) between the ultimate responsible officer at the Client and the Supplier's operations manager.

For every escalation, the following are stated as a minimum: the nature of the incident, the impact, possible solutions (if known), the actions initiated and the expected delivery time (if known).

Contact details for escalation:

- Support Center (step 1): 088 888 4222, on working days 9am – 5pm (Dutch time);
outside office hours (weekdays between 5pm and 9am Dutch time, and weekends) for Prio 1 incidents: 088 888 4200.
- Account manager (step 2): 088 888 4244.
- Operations manager (step 3): 088 888 4288.

2.6.3 Reporting of escalations

All arrangements made during the escalation procedure are recorded and sent by e-mail to the participating parties at that escalation level. The content corresponds to the ticket, supplemented by the solution chosen, its impact and the planned follow-up actions and lead times.

2.6.4 Evaluation of escalations

Escalations are evaluated during the meetings with the account manager at tactical level. The tickets and the reports drawn up form the input for these discussions.

3 Data Processing Agreement

This part describes how the Supplier, as processor, handles the personal data entered by the Client as controller, in accordance with the GDPR.

3.1 Data Processing Agreement Fortes Change Cloud

The Supplier processes personal data for and on the instructions of the Client. The General Data Protection Regulation (GDPR) therefore qualifies the Supplier as a 'processor' and the Client as a 'controller'. The GDPR requires the Supplier and the Client to conclude a data processing agreement. Because the Supplier provides a standard application (Fortes Change Cloud) and standard services, the data processing agreement has been incorporated into these General Terms and Conditions and Service Agreement. The definitions used are aligned with the GDPR. The Supplier processes personal data solely on the instructions of the Client and in order to perform the agreement.

3.1.1 Processing instructions

The processing by the Supplier consists of making its applications available, containing the data entered and generated by the Client. The Supplier does not add, modify or delete any data without written instructions. The Client can give such instructions by means of a request or via the application.

Within the Supplier's software, the Client can record various types of personal data. The Supplier understands that the Client may enter all of these personal data or categories, as well as any it creates itself, and that the Supplier subsequently processes these. The Client is itself responsible for assessing whether the purpose and nature of the processing are compatible with the Supplier's services.

The Supplier collects data about the use of its products. This data helps the Supplier to gain insight into whether, how and how often certain parts of the product are used. The Supplier can use this data to improve its products and services. The Supplier will not use this data for any other purpose or make it available to third parties. The Supplier will not provide the Client's data to third parties without the Client's express consent. The Supplier may, however, provide the Client's data to third parties in so far as it is required to do so under statutory provisions. The Supplier takes various measures to protect customer data as effectively

as possible. Through the use of both administrative and technical systems, only authorised users have access.

All customer data is stored separately for each Client. Only the Supplier's administrators are able to obtain access to all customer data. The data centres housing the Supplier's servers are located exclusively within the EEA, meet the strictest physical security requirements and fall entirely within the Dutch and European legal order.

3.1.2 Duty of confidentiality

The Supplier is aware that the information the Client shares with the Supplier and stores within Fortes Change Cloud is confidential and commercially sensitive in nature. The Supplier's employees handle the Client's information responsibly, as laid down in their employment contracts, which include a confidentiality clause.

3.1.3 Privacy rights

The Supplier has no control over the personal data made available by the Client. Without the Client's express consent or a statutory obligation, the Supplier does not provide any data to third parties. Nor does the Supplier process the data for purposes other than those agreed. The Client warrants that the personal data may be processed on the basis of a legal ground referred to in the GDPR. To the extent required, the Client's auditors (internal or external), or auditors engaged by the supervisory authority, may carry out audits to verify whether the Supplier complies with the terms and provisions of the agreement, supervisory rules and/or applicable mandatory legislation. The Supplier informs the Client of any such audit as soon as possible, unless this is prohibited.

3.1.4 Data subjects

The Client is itself responsible for the data entered relating to data subjects and for informing and assisting data subjects in exercising their rights. The Supplier never responds to requests from data subjects itself and always refers them to the Client as controller. If a data subject exercises its rights under the GDPR or other applicable regulations, the Supplier assists the Client, in so far as this is possible within the application, so that the Client can comply with its statutory obligations.

3.1.5 Security

The Supplier does everything it can, at a technical and organisational level, to protect the Client's personal data against loss or other unlawful processing. The Supplier is ISO 27001 certified. These measures form the basis for an appropriate level of security in line with the GDPR. The Supplier always assists the Client in properly fulfilling its obligations under the GDPR and other laws and regulations. By agreement, the Client may have an audit carried out during the term of the agreement; this is done at the Client's own expense.

The Supplier is liable for damage in relation to personal data caused by acts or omissions of the Supplier or the sub-processor. The limitation of liability set out in the Liability part applies in this respect. The Supplier cannot invoke a limitation of liability in the case of a recourse action under Article 82 of the GDPR.

If the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) issues a binding instruction to the Client, the Client will report this to the Supplier immediately. The Supplier will then do everything possible to achieve compliance. If the Supplier fails to do so and a fine is imposed, or if the AP imposes a fine directly on account of intent or gross negligence on the part of the Supplier, the limitation of liability set out in the Liability part does not apply.

3.1.6 Sub-processors

The Supplier processes customer data in the data centres of its hosting partner Root B.V. (Chamber of Commerce no.: 92479936, Enschede). The data centres are located exclusively in the Netherlands and are subject to Dutch laws and regulations. They comply with the strict Dutch and European legislation on logical and physical access security and continuity and are ISO 27001 certified as a minimum. The (personal) data is processed by the Supplier and this sub-processor exclusively within the European Economic Area. The same obligations apply to the Supplier and its sub-processor(s). An up-to-date overview of the sub-processors engaged by the Supplier is available via the Customer Support Portal.

In the optional Premium Edition of Fortes Change Cloud, the Supplier uses Power BI Embedded (a Microsoft Azure service) to deliver management dashboards. These are delivered from Microsoft data

centres in Western Europe. Microsoft Ireland Operations Ltd (registration no.: IE8256796) is therefore also a sub-processor.

The Supplier will not allow new sub-processors to process data without informing the Client in good time (at least 4 weeks in advance). The Client may at any time object to a sub-processor with the Supplier. The Supplier deals with such objections at board level. If the Supplier nevertheless allows the new sub-processor to process data, the Client may terminate the agreement with immediate effect.

3.1.7 Obligation to report data breaches

If it transpires that a data breach has occurred at the Supplier (within the meaning of Article 33 of the General Data Protection Regulation) that the Client must report to the Dutch Data Protection Authority and/or the data subject(s), the Supplier will inform the Client as soon as possible after the Supplier becomes aware of the data breach. The Supplier will endeavour to provide the Client immediately with all the information the Client needs in order to make a complete notification to the Dutch Data Protection Authority and/or the data subject. If this information is not yet known (for example because the data breach is still being investigated by the Supplier), the Supplier will provide the Client with the information the Client needs in order at least to make an initial provisional notification to the Dutch Data Protection Authority and/or the data subject.

If the Client makes a (provisional) notification to the Dutch Data Protection Authority and/or the data subject(s) about an alleged data breach at the Supplier, while it is reasonably clear that no data breach within the meaning of Article 33 of the GDPR has occurred at the Supplier, the parties will consult as soon as possible about the notification and any correction or withdrawal thereof. Unnecessary costs demonstrably incurred by the Supplier as a result of such an unwarranted notification may reasonably be charged on.

The Supplier requests that, if the Client makes a (provisional) notification to the AP and/or the data subject(s) about a data breach at the Supplier, the Client first informs the Supplier. This enables the parties to take the right decisions together about the actions to be taken.

Determining a data breach. In determining whether there has been a personal data breach, the Supplier uses the GDPR and the Dutch Policy Rules on the obligation to report data breaches as a guideline.

Notification to the Client. If a security incident or data breach occurs at the Supplier, the Client will be informed as soon as possible after the Supplier becomes aware of it. To achieve this, all of the Supplier's employees can report a data breach via the internal procedure (workflow). The Supplier also expects its sub-processors to assist in this respect. For the avoidance of doubt: the Supplier will of course also report a data breach at a sub-processor. In that case, the Supplier is the point of contact for the Client.

Notification period. In the event of a security incident or data breach, the Supplier will inform the Client as soon as possible, and no later than within 48 hours of discovery. The Client then assesses whether there is a data breach that must be reported to the Dutch Data Protection Authority and/or the data subject(s). The statutory 72-hour notification period (Article 33 GDPR) starts to run as soon as the Client becomes aware of the data breach; in practice, the moment at which the Supplier has informed the Client. The Supplier will provide the information the Client needs for a (provisional) notification as soon as possible.

Providing information. The Supplier will always endeavour to give the Client immediately all the information needed for any notification to the AP and/or the data subject(s).

Progress and measures. The Supplier informs the Client of progress and the measures taken. The Supplier makes arrangements about this with the primary contact person for the report. In any event, the Supplier keeps the Client informed if the situation changes, if there is additional information and about the measures being taken. The Supplier records all security incidents and handles them via a fixed procedure (workflow). The Supplier verifies the recording and handling of security incidents by means of an audit for ISO 27001 certification.

3.1.8 Deleting data

After the agreement ends, the Supplier deletes all customer data within 30 days, as set out in 'Termination of the agreement'. The Client may submit a request to have data deleted sooner; the Supplier is then obliged to do so.