Features of FACT24 ENS+ starter

Valid for new customers as from 22.05.2023

FACT24 ENS+ starter

FACT24 ENS+ Functionalities for Emergency Alerts

Activation

In an emergency, fast, safe and automatic alerts are important.

START AND STOP ALARM

You can use the FACT24 ENS+ web portal to start, monitor and stop alarms at any time; persons who have not yet been contacted will not receive any notification.

TEMPORARY ALARM MODIFICATIONS

Temporarily change your alarm configuration for the activation. All temporary modifications are only valid one time. The changes are not saved and do not change the default configuration of the alarm.

VIA TELEPHONE

A desired alarm can be triggered by a telephone call. You can start an alarm in silent mode, require a PIN or record a dynamic message.

QUICKSTART TELEPHONE

Accelerate the activation of an alarm with a "Quickstart". The desired alarm can be triggered by a telephone call. The activator of the alarm is identified by phone number.

Alarm End Devices

The alert can be go out via various end devices, which can be flexibly configured for persons and alarms.

END DEVICE CONFIGURATION

You can create five end devices per person:

- telephone,
- mobile phone,
- SMS,
- e-mail.

FACT24 PUSH NOTIFICATIONS

Push notifications are announced by a unique beep sound and displayed on your smartphone. Alarms can be confirmed immediately.

Alarm Modes

With our comprehensive alert solution, messages and acknowledgment options can be configured flexibly.

UNIDIRECTIONAL AS A MESSAGE

You can create five alarm scenarios and transmit information as a message. This can be done by push notification, phone, mobile phone and e-mail.

BIDIRECTIONAL WITH FEEDBACK

Information can also be transmitted as an alert with request for confirmation or time to location. The recipients can respond by phone, app, SMS, or e-mail with a web link.

Alarm Settings

Our system is flexible so that you can be too! Adjust the communication settings according to your needs.

STATIC ALERT

By default, people are addressed statically through group and personal relationships. Determine which people belong to a group and which characteristics they flag in the event of an alert.

MESSAGE SCOPE

You can create “fixed” messages with exact content and file attachments as well as variable messages, which are specified in an emergency.

FACT24 ENS+ starter

SELECTABLE MESSAGE LANGUAGES
There are 10 languages available: AR, DE, EN, ES, FR, IT, NL, PT, SV, RU. The communication language can be selected for message templates, in alarms, and for persons and users.

GROUP SPECIFIC DEVICE USE
Restrict which end devices should be used for a person in a specific group if necessary.

LAUNCH FORM
Simplify the launch of alarms by asking the user pre-configured questions. Based on the responses, the right alarm with tailored information will be triggered.

Alarm Procedures

Control the alert as you wish and send notifications in a targeted manner.

ALARM GOALS AND LOOPS
Set alarm-specific goals for number of persons to be reached. Define alarm loops if the alarm goal is not reached.

Occupational Health and Safety

Ensure the security of your people with the support of smart alerting processes.

LONE WORKING
FOR AN ADDITIONAL CHARGE

Lone worker solution, which is easy to implement and provides reliable personal security.

LONE WORKER DASHBOARD
FOR AN ADDITIONAL CHARGE

The Lone Worker Dashboard is used to display and monitor lone workers and alarms of lone workers.

Reports & Statistics

Interim and Alarm Reports give you information about the alarm history and valuable insights for the emergency and the future.

INTERIM AND FINAL REPORTS
Be informed automatically about the alert progression vie e-mail or webhook. Interim reports are sent after each completed escalation step and are a valuable basis for making decisions on how to proceed. Final reports are sent after the alarm has ended.

ALARM REPORTS
Alarm reports provide you a documentation of all alarms including responses received. Alarms are saved in reports up to 180 days.

ONLINE MONITOR
On the Online Monitor, you can view and track details about the alert procedure and it provides information on acknowledgments received.

FACT24 ENS+ starter

FACT24 System Administration and Security

Administration

Illustrate your business structure and decide what roles and rights each user has.

ADMINISTRATION LANGUAGES

Available administration languages FACT24 ENS+: CA, DE, EN, ES, FR, IT, NL, NO, PT; available administration languages FACT24 CIM: DE, EN, ES, FR

CONFIGURATION UPLOAD/DOWNLOAD

Upload and download the configurations of your persons, groups, annual calendar and duty rosters as an CSV file.

ASSIGNMENT OF ROLES AND RIGHTS

Complex corporate structures can be mapped thanks to detailed user, role and rights management.

Data Synchronisation

Various interfaces and connectivity options facilitate data synchronisation with FACT24.

MANUALLY USING EXCEL

You can manually upload a prepared Excel list (csv format) to have your data available in FACT24.

Support Services

We give you personal support every day with our decades of expertise.

FACT24 HELP PORTAL

In the FACT24 Help Portal, you can find answers to many product-related questions.

8/5 LOCAL CUSTOMER SUPPORT

Your F24 contact persons will be at your side during office hours (from 9am to 5pm CET).

ON-PAGE HELP

A format and plausibility check of the data facilitate data entry and alarm activation.

Security and Certification

A proven safety concept as well as regular penetration tests and re-certifications ensure guaranteed availability.

SECURITY CONCEPT

Data transfer is encrypted (transport layer security). Every year, all services are subjected to penetration tests by Syss GmbH, which is renowned throughout Europe.

MINIMUM AVAILABILITY

We guarantee the minimum availability of our services by contract.

- FACT24 Alerting Service: 99.99 %
- FACT24 ENS+ Web Administration: 99.50 %
- FACT24 Web Service Interface: 99.50 %
- FACT24 CIM Web Administration: 99.50 %

REDUNDANCY

Our sophisticated backup concept includes a redundant structure along the entire process chain (locations — systems — network providers).

CERTIFICATION

F24 AG became the first company in the world to be certified by The British Standards Institution (BSI) in 2010 for its integrated Information Security Management System (ISMS) and Business Continuity Management System (BCMS). For critical business processes, there is an integrated management system in accordance with the international standards ISO/IEC 27001:2013, ISO 22301:2019. An annual review and re-certification every three years ensures compliance with these international standards.

Features of FACT24 CIM starter

Valid for new customers as from 22.05.2023

FACT24 CIM starter

FACT24 CIM Functionalities for Crisis Management

Crisis Readiness

Save your BCM plans, alarm scenarios, and templates that are required in case of an emergency.

FILE ARCHIVE

Files and documentation can be saved and managed in individual folders in the File Archive, including version control. ALL of your plans are located in ONE place and can also be accessed if your own IT environment is not available. The File Archive contains storage space of 20 GB.

PRE-DEFINED ACTION CARDS

Use Action Cards to carry out your plans! Action Cards are predefined checklists that are automatically activated when registering the incident, depending on the role, type of incident and severity.

REPORT TEMPLATES

Customisable templates and forms can be used to log every type of meeting and to create reports (e.g. Situation Report). FACT24 CIM is delivered standard with best practices templates.

EXERCISE MODE

Do training about the emergency with the Exercise Mode so that all key personnel can familiarise themselves with the tool as well as a possible procedure. The Exercise Mode also has the advantage that this type of test area is separated from normal mode.

Mobilisation Crisis Staff

The combination of extensive alert and crisis management functions makes it easy to notify your persons and contacts.

MOBILISATION BY ALARMS

Immediately activatable alarms can be prepared with enough time beforehand using the extensive functionalities of FACT24 ENS+. With one click, these predefined alarm scenarios are ready for call-up. In the event of an emergency or crisis, a large number of people can be quickly notified. You can keep an eye on everything with the Online Monitor.

REGISTRATION OF INCIDENTS

Register new incidents with description, classification regarding type, phase and severity, as well as appendices. Additional custom fields can be added. Access can be restricted based on roles or users. All the follow-up information entered in the system is associated with an incident.

Crisis Handling

Your plans are implemented and form the basis for a successful virtual collaboration, which is logged continuously.

INCIDENT WORKSPACE

Here you can find all the information about an incident: details, such as the description, classification and display on the map, as well as Action Cards with status. You can also access the File Archive, generate reports, and trigger alarms.

AUTOMATIC RUNNING LOG

Registration of an incident automatically starts continuous logging. All information, decisions and actions are entered automatically. The documentation can be exported as an audit-proof PDF file.

FACT24 CIM starter

CASE MANAGER
A Case is used for quick and easy communication exchange and can be linked to an existing Incident. Up to 150 participants can be added to a case. Automatic logging takes place in the Running Log. Messages can be assigned a category before they are sent.

ACTION CARDS
In a crisis, you can benefit from prepared checklists in the form of Action Cards that you can follow for orientation. Action Cards are automatically activated depending on the role, type of incident and severity. Actions can be marked as completed, commented on, or assigned as a task.

STATUS MEETINGS
Almost every kind of meeting must be organised and carried out, including extra meetings and day-to-day events. Thanks to your pre-defined templates, you can log status meetings in the system in a structured and easy way, including the approval process.

Crisis Debriefing

Log file and statistics give you information about the course of the crisis and valuable insights for the future.

AUDIT-PROOF RUNNING LOG
The detailed log of each incident can be downloaded as an audit-proof PDF file and provides an overview of all actions and decisions.

SITUATION REPORT
Work together to create the Situation Report, get comments from teams in other locations, and get approval before submitting the report to executives.

TASK MANAGEMENT
Tasks offer individual response options, can be supplemented by file attachments and clearly displayed on a kanban board. Users with the corresponding authorisation can create tasks and assign them to other users, positions and experts outside the system.

OVERVIEW OF ALL INCIDENTS
A structured information view displays all active incidents with the most important information, such as reporting date and time, type and rating, and source. Each incident has a map view.

FACT24 CIM starter

FACT24 ENS+ Functionalities for Emergency Alerts

All advanced FACT24 ENS+ Functionalities are included in the FACT24 CIM Editions.

Activation

In an emergency, fast, safe and automatic alerts are important.

START AND STOP ALARM

You can use the FACT24 ENS+ web portal to start, monitor and stop alarms at any time; persons who have not yet been contacted will not receive any notification.

TEMPORARY ALARM MODIFICATIONS

Temporarily change your alarm configuration for the activation. All temporary modifications are only valid one time. The changes are not saved and do not change the default configuration of the alarm.

WITH THE APP

Alarms can be activated on the go, existing scenarios can be temporarily adjusted depending on the situation, and all activated alarms can be tracked via real-time monitoring.

VIA PC CLIENT

FOR AN ADDITIONAL CHARGE

Grant rights to persons to trigger specific alarms directly from their desktop.

VIA TELEPHONE

A desired alarm can be triggered by a telephone call. You can start an alarm in silent mode, require a PIN or record a dynamic message.

VIA WEBHOOK

Automated triggering of alarm is possible based on own programming via Webhook.

AUTOMATED VIA WEB SERVICES API

Automated triggering of alarm is possible based on own programming via the Web Services API.

SCHEDULED ALARM START

A scheduled activation can be particularly useful for periodic alerts as well as for test alarms for exercise purposes.

INDIVIDUAL DIAL-IN PHONE NUMBER

2 INCLUSIVE

An Individual dial-in phone number can either be used as International Emergency Number or as an Information Hotline.

INDIVIDUAL EMERGENCY NUMBER

When calling an individual emergency number, a pre-prepared alarm starts automatically. Thereby, the caller can be directly connected to a conference call together with all persons assigned to the alarm. Also, alarms can be triggered in silent mode (without the caller being asked for any information). An individual dial-in number is required to use this functionality.

INFORMATION HOTLINE

With the FACT24 Info Hotline, you can set up a public telephone hotline at short notice. This allows you to quickly notify a large number of external callers with up-to-date messages about an event. An individual dial-in number is required to use this functionality.

FACT24 CIM starter

QUICKSTART E-MAIL & SMS

Automated alarm activation is also possible via e-mail and SMS. Content such as the subject and text are processed as part of variable message and forwarded via all alert channels.

QUICKSTART TELEPHONE

Accelerate the activation of an alarm with a "Quickstart". The desired alarm can be triggered by a telephone call. The activator of the alarm is identified by phone number.

Alarm End Devices

The alert can be go out via various end devices, which can be flexibly configured for persons and alarms.

END DEVICE CONFIGURATION

You can create 16 end devices per person of the following types:

- telephone,
- mobile phone,
- SMS,
- e-mail,
- fax,
- pager,
- app,
- MS Teams
- and PC Client if booked.

FACT24 PUSH NOTIFICATIONS

Push notifications are announced by a unique beep sound and displayed on your smartphone. Alarms can be confirmed immediately.

DESKTOP ALERTING

FOR AN ADDITIONAL CHARGE

Receive alerts as pop up on desktop via PC Client.

MICROSOFT TEAMS INTEGRATION

Receive alerts as messages in Microsoft Teams.

Alarm Modes

With our comprehensive alert solution, messages and acknowledgment options can be configured flexibly.

UNIDIRECTIONAL AS A MESSAGE

You can create unlimited alarm scenarios and transmit information as a message. This can be done by push notification, phone, mobile phone, e-mail fax and pager.

BIDIRECTIONAL WITH FEEDBACK

Information can also be transmitted as an alert with request for confirmation or time to location. The recipients can respond by phone, app, SMS, or e-mail with a web link.

ALARM CHAT

Activate alarm chat to allow quick emergency communication between all recipients via mobile app and portal. Chat supports up to 150 participants.

ADVANCED FEEDBACK OPTIONS

Define individual confirmation options or ask recipient to work through a task list (available via app).

FACT24 CIM starter

AUTOMATIC CONFERENCE START
Automatically start a conference call with an alarm. The contacted persons are invited to this conference during the alert procedure, and the activator of the alarm can be brought in.

Alarm Settings

Our system is flexible so that you can be too! Adjust the communication settings according to your needs.

STATIC ALERT
By default, people are addressed statically through group and personal relationships. Determine which people belong to a group and which characteristics they flag in the event of an alert.

MESSAGE SCOPE
You can create “fixed” messages with exact content and file attachments as well as variable messages, which are specified in an emergency.

MESSAGE TEMPLATES
Prepare message templates to re-use them for multiple alarms or across the organisation.

SELECTABLE MESSAGE LANGUAGES
There are 10 languages available: AR, DE, EN, ES, FR, IT, NL, PT, SV, RU. The communication language can be selected for message templates, in alarms, and for persons and users.

RECIPIENT LEGITIMATION (PIN)
You can use a PIN request as a security measure so that only persons who are authorised with PIN receive the messages via the end device telephone.

GROUP SPECIFIC DEVICE USE
Restrict which end devices should be used for a person in a specific group if necessary.

OUTBOUND LOCATION-BASED ALERTING
Alert people based on their location.

INBOUND LOCATION-BASED ALERTING
Trigger the correct alarm depending on the location of the alarm trigger.

QUALIFICATION-BASED ALARM GOAL
When a qualification-based alarm goal is set, only people with the necessary primary skill are requested.

FILTER-BASED ALERTING
Filter all persons flexibly by language, profile, organizational unit, group memberships, primary qualification, and 30 additional qualifications to make sure you reach out to the right audience at the time of alarm triggering, even in large organizations with constant change.

CALENDAR-BASED ALERTING
Set time-based rules to alert different groups or to start another alarm depending on the time the alarm is triggered.

CUSTOM VOICE PROMPTS
For voice channels, you can overwrite the voice engine's default welcome, confirmation, goodbye, and cancel texts with your individual text.

LAUNCH FORM
FOR AN ADDITIONAL CHARGE

Simplify the launch of alarms by asking the user pre-configured questions. Based on the responses, the right alarm with tailored information will be triggered.

DUTY ROSTER
Organise a duty roster to assign individual persons with one or more time periods/ shifts to the on-duty service within an alarm flow.

VISUALISER
Custom interface to trigger and monitor alarms, which you can design based on your organisation's needs.

Alarm Procedures

Control the alert as you wish and send notifications in a targeted manner.

ADVANCED ALARM TYPES
Choose between parallel, channel-based, device-based and serial alarms. Define, for example, that people who are sent an alarm first receive a text message and then a call two minutes later, or people should be alarmed one after the other instead of all at once.

ALARM GOALS AND LOOPS
Set alarm-specific goals for number of persons to be reached. Define alarm loops if the alarm goal is not reached.

ESCALATION
If the alarm goal is not reached, define alternative persons and groups (including personal deputies) as escalation process.

EXTENDED ALARM ESCALATION
If the alarm goal is not reached via loops and escalation to other persons and groups, extend the escalation to alternative alarms.

DYNAMIC GROUPS
Create dynamic groups for an alarm, i.e., temporary groups for people who have already been alerted and confirmed positively or rejected, so you can send them additional information.

Occupational Health and Safety

Ensure the security of your people with the support of smart alerting processes.

LONE WORKING
FOR AN ADDITIONAL CHARGE

Lone worker solution, which is easy to implement and provides reliable personal security.

LONE WORKER DASHBOARD
FOR AN ADDITIONAL CHARGE

The Lone Worker Dashboard is used to display and monitor lone workers and alarms of lone workers.

FACT24 CIM starter

Reports & Statistics

Interim and Alarm Reports give you information about the alarm history and valuable insights for the emergency and the future.

INTERIM AND FINAL REPORTS

Be informed automatically about the alert progression vie e-mail or webhook. Interim reports are sent after each completed escalation step and are a valuable basis for making decisions on how to proceed. Final reports are sent after the alarm has ended.

ALARM REPORTS

Alarm reports provide you a documentation of all alarms including responses received. Alarms are saved in reports up to 5 years.

ONLINE MONITOR

On the Online Monitor, you can view and track details about the alert procedure and it provides information on acknowledgments received.

STATISTICS

Based on different filter options various statistics, such as average response time per alarm or most triggered alarms can be displayed.

FACT24 CIM starter

FACT24 System Administration and Security

Administration

Illustrate your business structure and decide what roles and rights each user has.

ADMINISTRATION LANGUAGES

Available administration languages FACT24 ENS+: CA, DE, EN, ES, FR, IT, NL, NO, PT; available administration languages FACT24 CIM: DE, EN, ES, FR

CONFIGURATION UPLOAD/DOWNLOAD

Upload and download the configurations of your persons, groups, annual calendar and duty rosters as an CSV file.

PROFILES FOR PERSONS

Grant persons the right to trigger select alarms via mobile app or PC client (if booked).

TWO-FACTOR AUTHENTICATION

Increase security by using Two-factor Authentication. You will receive a code via SMS that must be entered to log in. Defined password criteria provide additional security.

DOCUMENT MANAGEMENT

Provide relevant documents to your recipients which will also be available offline via app.

ASSIGNMENT OF ROLES AND RIGHTS

Complex corporate structures can be mapped thanks to detailed user, role and rights management.

CONTACT DATA MANAGEMENT BY EMPLOYEE

Send your employees an e-mail to update contact information. This allows each person to update their own data.

EXTENDED PROFILES FOR PERSONS

Grant persons additional rights to self-checkin and out of groups and access select emergency documents.

MAPPING OF COMPLEX ORGANISATIONS

- Single account: 10 users, 1 Organisational Unit
- Multiple account: 250 users, 10 Organisational Units
- Corporate account: 1,000 users, 100 Organisational Units

Data Synchronisation

Various interfaces and connectivity options facilitate data synchronisation with FACT24.

MANUALLY USING EXCEL

You can manually upload a prepared Excel list (csv format) to have your data available in FACT24.

VIA F24 SFTP SERVER

FOR AN ADDITIONAL CHARGE

We also offer data synchronisation (csv, xml, other formats on request) via the F24 SFTP server for an additional charge.

AUTOMATED VIA WEB SERVICES API

Automated synchronisation of the data is possible based on own programming via REST API.

SSO IDENTIFIER VIA SAML PROTOCOL

Simplify your identity and access management. Own configuration required.

Support Services

We give you personal support every day with our decades of expertise.

FACT24 HELP PORTAL
In the FACT24 Help Portal, you can find answers to many product-related questions.

ON-PAGE HELP
A format and plausibility check of the data facilitate data entry and alarm activation.

8/5 LOCAL CUSTOMER SUPPORT
Your F24 contact persons will be at your side during office hours (from 9am to 5pm CET).

24/7 CUSTOMER SUPPORT
FOR AN ADDITIONAL CHARGE

For urgently needed support, we are also available outside office hours (from 9am to 5pm CET) in English.

Security and Certification

A proven safety concept as well as regular penetration tests and re-certifications ensure guaranteed availability.

SECURITY CONCEPT
Data transfer is encrypted (transport layer security). Every year, all services are subjected to penetration tests by Syss GmbH, which is renowned throughout Europe.

REDUNDANCY
Our sophisticated backup concept includes a redundant structure along the entire process chain (locations — systems — network providers).

MINIMUM AVAILABILITY
We guarantee the minimum availability of our services by contract.

- FACT24 Alerting Service: 99.99 %
- FACT24 ENS+ Web Administration: 99.50 %
- FACT24 Web Service Interface: 99.50 %
- FACT24 CIM Web Administration: 99.50 %

CERTIFICATION
F24 AG became the first company in the world to be certified by The British Standards Institution (BSI) in 2010 for its integrated Information Security Management System (ISMS) and Business Continuity Management System (BCMS). For critical business processes, there is an integrated management system in accordance with the international standards ISO/IEC 27001:2013, ISO 22301:2019. An annual review and re-certification every three years ensures compliance with these international standards.

FACT24
an F24 product

	FACT24 ENS+			FACT24 CIM		
	starter	essential	advanced	starter	essential	advanced
CAPACITY						
USER CAPACITY						
Single Account (1 Organisational Unit)	10	10	10	25	25	25
Multiple Account (up to 10 Org. Units)			250	250	250	250
Corporate Account (up to 100 Org. Units)			1.000	1.000	1.000	1.000
FUNCTIONAL CAPACITY						
Alarm Scenarios [1]	5	99	?	?	?	?
Devices per Person	5	16	16	16	16	16
Number of Groups	20	?	?	?	?	?
Telephone Conference Participants	n/a	30	60	60	60	60
ENS+ Alarm report availability	max. 1 year	max. 2 years	max. 5 years	max. 5 years	max. 5 years	max. 5 years
FACT24 CIM FOR CRISIS MANAGEMENT						
CRISIS READINESS						
File Archive				■	■	■
Pre-defined Action Cards				■	■	■
Report Templates				■	■	■
Exercise Mode				■	■	■
Risk Management						■
MOBILISATION OF CRISIS STAFF						
Using Alarms	■	■	■	■	■	■
Incident Register				■	■	■
↳with additional custom fields						■
Through automatic incident creation via API					■	■
CRISIS HANDLING						
Crisis Management on the Go				■	■	■
Incident Workspace				■	■	■
Automatic Running Log				■	■	■
Via Case Manager				■	■	■
Situation Report				■	■	■
Action Cards				■	■	■
Task Management				■	■	■
Status Meetings				■	■	■
Overview of all Incidents				■	■	■
With preconfigured Information Boards					■	■
Over 3 levels: strategic/tactical/operational					■	■
Map with linked locations					■	■
Handling of Media enquiries						■
Persons of Concern Management						■
CRISIS DEBRIEFING						
Audit-proof Running Log				■	■	■
Incident Statistics					■	■

FACT24
an F24 product

	FACT24 ENS+			FACT24 CIM		
	starter	essential	advanced	starter	essential	advanced
FACT24 ENS+ FOR EMERGENCY NOTIFICATION						
ACTIVATION						
Start and Stop Alarm	■	■	■	■	■	■
Temporary Alarm Modification	■	■	■	■	■	■
With the App		■	■	■	■	■
Quickstarts Telephone	■	■	■	■	■	■
Quickstarts E-Mail & SMS		Add-on	Add-on	■	■	■
Via PC Client			Add-on	Add-on	Add-on	Add-on
Via Telephone	■	■	■	■	■	■
Via Webhook		■	■	■	■	■
Via Web Services API		Add-on	Add-on	■	■	■
Scheduled alarm start		■	■	■	■	■
Individual dial-in phone number		Add-on	2 inclusive	2 inclusive	2 inclusive	2 inclusive
ALARM END DEVICES						
Telephone/Mobile Phone, SMS, E-Mail	■	■	■	■	■	■
Pager and Fax		■	■	■	■	■
FACT24 Push Notifications	■	■	■	■	■	■
Desktop Alerting			Add-on	Add-on	Add-on	Add-on
Microsoft Teams Integration		Add-on	Add-on	■	■	■
ALARM MODES						
Unidirectional as a Message	■	■	■	■	■	■
Bidirectional with Feedback Function	■	■	■	■	■	■
Alarm chat		■	■	■	■	■
Automatic Conference Start		■	■	■	■	■
Advanced feedback options			■	■	■	■
ALARM SETTINGS						
Static Alert	■	■	■	■	■	■
Message scope fixed/variable	■	■	■	■	■	■
Message Templates		■	■	■	■	■
Selectable Message Languages (9)	■	■	■	■	■	■
Recipient ID (PIN request)		■	■	■	■	■
Group Specific Device Use	■	■	■	■	■	■
Outbound Location-based Alerting		■	■	■	■	■
Inbound Location-based Alerting			■	■	■	■
Qualification-based Alarm goal		■	■	■	■	■
Filter-based Alerting			■	■	■	■
Calendar-based Alerting		■	■	■	■	■
Duty Roster			■	■	■	■
Custom voice prompts			■	■	■	■
Visualiser		Add-on	Add-on	■	■	■
Launch form	Add-on	Add-on	Add-on	Add-on	■	■

	FACT24 ENS+			FACT24 CIM		
	starter	essential	advanced	starter	essential	advanced
FACT24 ENS+ FOR EMERGENCY NOTIFICATION (Continuation)						
ALARM PROCEDURES						
Advanced Alarm types		■	■	■	■	■
Alarm goals and loops	■	■	■	■	■	■
Escalation		■	■	■	■	■
Extended Alarm escalation			■	■	■	■
Dynamic Group			■	■	■	■
OCCUPATIONAL HEALTH AND SAFETY						
Lone Working	Add-on	Add-on	Add-on	Add-on	Add-on	Add-on
Lone Worker Dashboard	Add-on	Add-on	Add-on	Add-on	Add-on	Add-on
REPORT & STATISTICS						
Interim and Final Reports	■	■	■	■	■	■
Alarm Reports	■	■	■	■	■	■
Online Monitor	■	■	■	■	■	■
Statistics			■	■	■	■
FACT24 SYSTEMADMINISTRATION AND SUPPORT						
ADMINISTRATION						
Languages FACT24 CIM: DE, EN, ES, FR, NO				■	■	■
Languages FACT24 ENS+: CA, DE, EN, ES, FR, IT, NL, NO, PT	■	■	■	■	■	■
Assignment of Roles & Rights	■	■	■	■	■	■
Configuration Upload and -Download	■	■	■	■	■	■
Contact Data Management by Employee		■	■	■	■	■
Profiles for persons		■	■	■	■	■
Extended profiles for persons			■	■	■	■
Two-factor Authentification			■	■	■	■
Mapping of complex Organisations			■	■	■	■
Document management			■	■	■	■
DATA SYNCHRONISATION						
Manually with prepared Excel list	■	■	■	■	■	■
Automated via Web Services API		Add-on	Add-on	■	■	■
Via F24 SFTP-Server		Add-on	Add-on	Add-on	Add-on	Add-on
SSO Identifier via SAML protocol			■	■	■	■
SUPPORT SERVICES						
FACT24 Help Portal	■	■	■	■	■	■
On-page help	■	■	■	■	■	■
8/5 local Customer Support	■	■	■	■	■	■
24/7 Customer Support [2]		Add-on	Add-on	■	■	■

1) Accounts with up to 5000 persons can have 10, 25, or 50 active alarms in parallel, depending on their selected product edition (10 for ENS+ starter, 25 for ENS+ essential, and 50 from ENS+ advanced).

Accounts with more than 5000 persons can have 25, 50, or 100 active alarms in parallel, depending on their selected product edition (25 for ENS+ starter, 50 for ENS+ essential, and 100 from ENS+ advanced).

2) Please note that 24/7 Support outside of business hours, 9 am – 5 pm CET, is only available in English.

F24 AG
Technical and organisational measures pursuant to Article 32 GDPR

F24 operates an integrated management system for information security (“ISMS”) and a business continuity system (“BCMS”) which is certified by an independent, accredited institution, the “The British Standards Institution (“BSI Group”) based on the ISO/IEC 27001:2013 and ISO 22301:2019 international standards. The certifications apply to both F24 AG and most of our subsidiaries. In addition to annual surveillance reviews, re-certification is performed every three years.

The following technical and organisational measures are in place to guarantee protection of data and information security.

1. Confidentiality (Article 32(1)(b) GDPR)

- **Physical access control**
  F24’s FACT24 production systems are operated at several geographically segregated (cloud) data centres from different providers. Only authorised personnel are permitted to have physical access to the data processing centres. Access is only possible using a personalised magnetic card in combination with a PIN and/or biometric recognition. The data centres are equipped with security gates, have electric door openers and are subject to video surveillance. Access is logged electronically. Physical servers are operated in dedicated racks that may only be accessed by F24 operations staff. In addition, entry to cloud data centres is not possible as a rule – even by F24 staff – because they comprise a completely virtual solution that is operated autonomously by the provider. Organisational instructions are in place for issuing keys at the buildings where office operations are located, along with escorts for visitors. Rooms used for technical operations are protected via an alarm system, along with security personnel who perform patrols at regular intervals.
- **Systems access control**
  Unauthorised system use is not possible as a rule. The electronic data processing systems are outfitted with a central Identity Policy & Audit-System; log-in is only possible with personal multi-factor authentication. Work station computers for F24 staff are protected via an automated, password-protected screen lock. All data media containing customer information are encrypted using AES-XTS-256 (password with PBKDF2, „salted“, HMAC-SHA512). VPN tunnels – likewise on the basis of IPSEC (AES-256-SHA256 with at least 2048 bit) – are used for purposes of remote access to systems by F24 operations staff when support is needed. Personalised 2-factor authorisation processes are used exclusively. In addition, communications themselves are encrypted using Transport Layer Security (at least TLS 1.2). Customer data backups are also stored using AES-XTS-256 encryption. All TrustCase messages are encrypted with NaCL and XSALSA 20/20 (with a 256-bit key) both in the database and during transmission.
- **Personal access control**

Customers perform maintenance of existing data themselves via the FACT24 web interface. Here, too, password-protected and encrypted access (at least TLS 1.2) are used. A specific password policy may be configured so as to provide for different password criteria (upper case/lower case, letters, special characters, numbers, expiry date, minimum/maximum number of characters). Two-factor authentication may be activated as an option for access to FACT24. The respective IP address is blocked following several incorrect login attempts. A differentiated role/rights concept ensures that only persons who are appropriately authorised and trained may modify existing data. Access, roles and thus authorisations within the customer organisation are issued by the customer's privileged administrators. Only the user can re-set passwords. Upon request, an IP address range may be specified as a white list for purposes of data administration. After initial set-up for the customer, personal stock data for FACT24 services will only be entered, modified or erased by the customer themselves . All log-ins as well as activities – both on the system side and those that relate to FACT24 use – are logged on a personalised basis.
F24 staff only access customer data within the scope of providing support or maintenance. The need-to-know principle applies in such cases; only a limited group providing support has access in such cases. From an organisational standpoint, the approval of authorisations is segregated from setting up authorisations.

- **Separation controls**
  F24 ensures that data collected for different purposes is processed separately. On the one hand, such segregation is physical: Different data from different applications is stored on dedicated systems/computers; on the other hand, the segregated processing of application-related data is ensured by means of the data model and corresponding authorisation concepts ("multi-client capability"). The clients/accounts of customers are logically segregated on the FACT24 system.
  The F24 systems for product development, testing and quality assurance, as well as production, are physically segregated. Development and testing is not conducted using productive stock data. All F24 employees are obliged to maintain data secrecy and have signed appropriate declarations. Employees are regularly notified of new technical and legal developments and receive appropriate training.
- **Pseudonymisation** (Article 32 (1) (a) GDPR; Article 25 (1) GDPR)
  Data required for alert purposes is not pseudonymised because the customer works with this data in their account on the FACT24 system, and such data must be readable for the customer. ("In consideration of the ... context and purposes of processing...." Article 32 (1) GDPR). General log data (e.g. IP addresses on web servers, etc.) is anonymised after a period of seven days. Contact data in the TrustCase messaging app is determined solely by means of comparison of SHA-256 hashed telephone numbers.

2. Integrity (Article 32(1)(b) GDPR)

- **Transfer control**
  All data traffic for FACT24 services via the Internet is encrypted (at least TLS 1.2). No removable media are used for transport or transfer of sensitive data (e.g. personal data). External system access via defined interfaces (e.g. APIs) is likewise performed on an encrypted basis (at least TLS 1.2) and is comprehensively recorded. Support access is made solely via a VPN connection on an IPSEC basis (AES-256-SHA256 with at least 2048 bit). In this context, personalised 2-factor authorisation processes are used exclusively.
- **Input control**
  All actions and the respective operator (user account) are logged with date and time in an audit-compliant manner. In this context, both standard logging processes for the system environments (operation system, database) and logging mechanisms implemented specifically for FACT24 are used.

Every access to protected data is logged. Important log data is analysed on a regular basis during the contract phase and stored in accordance with applicable legal requirements. At the end of the contract, the customer has the option of erasing their data from the system itself. If the customer does not do so, data is fully erased after six months.

3. Availability and resilience (Article 32(1)(b) GDPR)

- **Availability control**
  F24 has an integrated management system for ISMS (Information Security Management System) and BCMS (Business Continuity Management System) certified under ISO 27001 and ISO 22301. The certifications apply to both F24 AG and most of our subsidiaries. Comprehensive measures are in place to ensure availability. Customer data is mirrored via multiple data centres and databases, all FACT24 service systems are multi-redundant and available via different provider access lines. In addition, backups are made at regular intervals and in turn stored in multiple data centres. All systems are equipped with firewalls, security zones and uninterruptible power supplies (UPS). The systems are scanned continuously for vulnerabilities, and the systems with customer access are also scanned with signature-based and heuristic virus scanners.
- **Prompt restoration** (Article 32(1)(c) GDPR);
  All customer data for all customers on FACT24 systems may be restored promptly using the backups. For this purpose, so-called snapshots of the databases are generated at regular intervals and stored as encrypted backups.

4. Process for regular testing, assessment and evaluation (Article 32(1)(d) GDPR; Article 25(1) GDPR)

- **Data protection management**
  atarax GmbH & Co. KG has been appointed as data protection officer. atarax specialises in all issues related to data protection and provides support to F24.
  In addition, so-called penetration tests for infrastructure and applications are performed at annual intervals by an independent, well-known security firm.
- **Incident Response Management**
  Within the scope of the certified integrated Business Continuity Management System, so-called Business Continuity plans have been prepared for risk scenarios that permit fast and efficient action in the case of any incidents.
- **Data protection by default** (Article 25(2) GDPR)
  F24 customers are provided an extensive introduction for the FACT24 system and its components. Options for data collection (e.g. contact data management) are discussed during this introduction. Customers operate and administer the FACT24 system and the customer data contained therein themselves. Accordingly, customers also determine how and to what extent they collect data from their employees. All default settings are data protection-friendly and designed for high levels of security; for example: services with an opt-in for users and a restrictive policy for strong passwords.
- **Commissioned data processing**
  The scope of commissioned data processing the customer instructs F24 to undertake pursuant to Article 28 GDPR is exclusively and clearly defined in the commissioned data processing contract. No additional processing is performed beyond this scope.

  The same strict standards that apply to F24 as a processing company apply to the choice of subcontractors and/or service providers for F24. Any such service providers are to be listed in the document “F24 Subcontractors under Article 28(2)-(4) GDPR”. The list may only be expanded with the express written consent of the controller. This provides the customer the opportunity to raise an objection (Article 28(2) GDPR).

F24 AG
FACT24 PROCEDURAL NOTIFICATION

Article 30 of the European Union General Data Protection Regulation (GDPR) requires that a record is kept of all processing activities. This procedural notice originating from F24 as the Processor pursuant to Article 30 II GDPR enables the Controller to prepare a record of processing activities in relation to the FACT24 service and additional supporting processes.

1. Processor

Name and address of the responsible entity	F24 AG, Ridlerstraße 57 80339 Munich Germany
Telephone / Fax	T: +49-89-2323638-0 F: +49-89-2323638-6
E-mail address	office@f24.com
Internet address / URL	www.f24.com

2. Legal representatives of the Processor

Board of Directors	Dr Jörg Rahmer, Christian Götz

3. Personal information and contact information for the data protection officer at Processor referred to under no. 1

Name	Atarax GmbH & Co. KG
Street address	Ridlerstraße 57
Postal code / City	80339 Munich, Germany
Telephone / Fax	T: +49-89-2323638-0 F: +49-89-2323638-6
E-mail address	dataprotection@f24.com

4. Purpose; Process description; Categories of processing

Purposes for which data is processed	F24 develops and operates highly secure telecommunications solutions for providing alerts and communications in emergencies and crisis situations. Using the FACT24 alert and crisis management service, F24 customers automatically alert their management crisis teams in the case of an emergency, can initiate ad hoc conference calls with the push of a button or activate an info hotline on short notice. Using the integrated secure messenger TrustCase, customers can send alerts and work together in virtual crisis rooms. In this context, specialists at F24 analyse the customer's communications needs when an event happens and support their users when mapping potential scenarios or provide assistance during implementation when using FACT24 or provide customer support. Data is collected, processed and used within the scope of fulfilling the purposes described above, so long as a contractual relationship is in place for the use of the FACT24 service. We offer "Guided Tours" for targeted support in the use of the FACT24 web interface. To provide these, we use an established technical solution from the German company Userlane GmbH. To be able to deliver Userlane, a connection is established between the

user's browser and Userlane, for which IP addresses are inevitably required. There is no storage of IP addresses.

Only applicable if contractual relationship covers A3M Global Monitoring: travel data is processed to enable location-based information and alerting if (i) manually entered by customer or (ii) automatically imported via booking tool (pre-requisite: dedicated DPA to be signed).

Only applicable if contractual relationship covers person data management by data upload via SFTP server or direct connection via middleware Orchestra by Soffico: person data is processed for the sole purpose to update person data in FACT24.

5. Groups of data subjects and data or categories of data affected

Description of the primary groups of data subjects affected	Employees, suppliers and additional business partners of customers who use FACT24, as well as additional stakeholders related to the fulfilment of the purposes referred to under no. 4.
Description of the primary related data or categories of data	These essentially comprise the data or categories of data listed below: **Users:** User name, password, contact information (telephone, e-mail, fax), address, location, role, organisational reference area, authorisations, status, logs of change to objects, language, additional information, IP address **Persons:** Number, organisational affiliation and its location, name, contact information (typically pager, telephone, fax and e-mail), language, optional qualifications within the scope of selection in an alert case, status, information regarding telephone standby service, information regarding contact data maintenance, assignment to shift groups, optional additions and comments, scheduled absences, PIN for recipient identification, access rights for crisis rooms, membership in groups to be alerted, responses in the case of alert confirmations, contributions within virtual crisis rooms, last dynamic location (optional with opt-in)
Special categories of personal data	Processing data within the context of the FACT24 process is intended to avoid or minimise material and/or non-material damages to persons and things as part of an incident and crisis management service. The purpose of the FACT24 process is not to evaluate the personality of persons included in the process. No data within the meaning of Article 9 GDPR is stored or processed as part of the FACT24 process.

6. Recipients or categories of recipients who may receive data

Public authorities if required by applicable laws and regulations. External contractors commissioned by F24 to perform data processing. Internal departments within the F24 Group in order to fulfil the purpose set out under no. 4.

7. Default time limits for the erasure of data

Data included within the FACT24 process is fundamentally input and erased by the data controller. Six months following the elimination of the purpose set out under no. 4, F24 independently erases customer data. During the term of the contract, log files from alert cases (alarm logs) are available for a period of two years for download by the client and are erased following this period.

8. Planned data transfers to third countries

The provision of contractually agreed data processing tasks may only take place within a member state of the European Union, or within a contracting state to the Agreement on the European Economic Area, or within a state, which has been recognised as providing an adequate level of data protection Beyond, there is no data transfer planned.

GENERAL TERMS AND CONDITIONS OF BUSINESS
for services of F24 AG – hereinafter referred to as F24

1. Area of Application

These Standard Business Terms apply to all business relationships between F24 and its customers. However, these Standard Business Terms only apply if the customer is an entrepreneur (section 14 German Civil Code - “BGB”), a legal person under public law or a special fund under public law.

2. Nature and scope of the services / Term of contract

2.1 The qualities, nature and scope of the services to be provided are set out in the respective service agreement and in relation to the eCall business SMS&FAX portal are set out in the eCall terms and conditions of use.

2.2 Unless otherwise agreed in writing, the term of contract for services of F24 shall be twelve (12) months. The contract shall be extended by a further twelve (12) months (extension period), unless it is terminated in writing three (3) months prior to the end of the contract term or the corresponding extension period. This shall not affect the right to termination without notice and the right to termination under subsection 5.2.

3. Reporting of Disturbance and Notification of Defects

The customer shall notify in writing or in text form (e.g. email or fax) any defects and disturbances of the services and systems of F24 immediately in detail and in an understandable manner.

4. Acts of co-operation

Acts of co-operation and supply by the Client that have been agreed or are necessary and expedient for performance of the contract, including those defined in the contract, shall be performed as essential contractual obligations of the Client. As part of its contractual ancillary obligations, F24 shall store data for the use of services and systems when reporting emergencies for a period of 24 months from the respective report and shall supply this information to the Client in electronic format on request. There are no other mutual obligations to store and supply such data.

5. Prices / Terms of Payment

5.1 Unless otherwise agreed in a specific case, the fees to be paid by the customer for the services may be found from the price list as applicable from time to time plus statutory value added tax and other statutory taxes, if any.

5.2 F24 reserves the right to make price adjustments for the services. In the event of price adjustment F24 will communicate the changed prices at least two months prior to the date they become effective. In case of price increases exceeding 5% within 12 months the customer will be entitled to terminate the contract in writing with one month’s notice upon receipt of the notification of the price increase to become effective on the price increase comes into force.

5.3 During any period of default, fees will be subject to interest at the applicable statutory late payment interest rate. F24 expressly reserves the right to assert claims for additional damage caused by delay.F24 will impose a dunning fee of EUR 15.00 from the second dunning notice.

5.4 The customer may not set off against claims unless for undisputed claims and such recognized by declaratory judgement, and may only assert a right to deny service or to withholding based on such a claim. This is without prejudice to the customer’s corresponding rights in the case of a defect.

5.5 Objections to the invoiced amount of fees depending on the volume of use of the services shall be notified in writing within 30 days upon receipt of the invoice. Failure to raise objections in due time will be deemed approval. In its invoice F24 will point out to the consequences of such failure to raise objections in a timely manner.

6. Use of Data

6.1 Personalized data communicated by the customer will be processed and used by F24 exclusively for the customer and according to its instructions (commissioned data processing). Any technical and organizational procedures for the processing and use of such personalized data exceeding the foregoing will be established by the customer upon consultation with F24. Costs and expenses in connection with the implementation of such procedures, if any, shall be paid by the customer to F24 on the basis of the price list as applicable from time to time.

6.2 The data protection regulations of the German Ordinance on Data Protection in the Telecommunications Industry and other applicable data protection laws and regulations will not be affected by the foregoing.

7. Defects and Disturbances

7.1 Liability for defects on the part of F24 is primarily based on agreements made with regard to the quality of the services. In the event quality has not been agreed, applicable legal provisions shall be applied to determine whether or not there is a defect. F24 assumes no liability for public comments made by third parties.

7.2 F24 will immediately inspect any notified defects of its services and initiate their removal, provided that F24 is obligated to remove defects.

7.3 The customer will be entitled to reduce payment due to defects if the customer notified – as defined in section 3 above – the specific defects which are the reason of reduction. Even in such a case reduction will only be permitted in proportion to the limitation of the options of use as a result of the notified defect.

7.4 Expenses for inspection and supplementary performance will be borne by F24 in the event there actually is a defect. However, if it is found to be the case that there is no defect and/or that the disruption was based on factors within the customer's scope of responsibility, F24 may demand reimbursement from the customer for costs resulting from the unjustified request to remedy a defect (including, in particular, inspection and travel expenses) unless the lack of a defect would not have been apparent to the customer based on a reasonable amount of effort.

7.5 The limitation period for claims based on defects of quality or defects in title of the services provided by F24 is one year from the start of the statutory limitations period. Section 548 (2) of the BGB *(German Civil Code)* will not be affected by the foregoing.

8. Liability

The liability of F24 for all the rights and claims resulting from and in connection with the conclusion and performance of the contract on services is – irrespective of the factual or legal ground – limited as follows, the provisions in section 7 above remaining unaffected:

8.1 In case of willful or fraudulent intent, claims under the German Product Liability Law, as well as injury of life, body and health, F24 will be liable in accordance with the legal regulations. In this context the limitations of liability below will not be applicable.

8.2 In case of gross negligence the liability of F24 is limited to the typical damages which were foreseeable for F24 at the time of entering into the contract. This limitation of liability will not be applicable in case of gross negligence of a legal representative or executive officer of F24.

8.3 In case of simple negligence F24 will only be liable to the extent as the damages were caused in breach of material contractual obligations, such liability being limited to the typical damages foreseeable for F24 at the time of entering into the contract. Material contractual obligations include such obligations that are essential to the proper performance of the contract and upon which the obligee has relied, and may also be expected to rely upon, and the culpable non-performance of which endangers achieving the purpose of the contract. Liability for typical, foreseeable damages is limited in amount to a maximum of EUR 500,000.00 for property damage and a maximum of EUR 500,000.00 for purely financial losses.

8.4 F24 will be liable under a guarantee accepted by F24 only to the extent as rights, claims and liability result from the explicit wording of the guarantee statement.

8.5 The customer's contributory fault, if any, will be taken into account accordingly.

8.6 In the absence of any other limitation of liability expressly agreed between the customer and F24, liability for typical, foreseeable damages is limited to maximum € 500,000.00. If the customer finds that the typical, foreseeable damage might exceed the above liability limits, the customer shall expressly draw the attention of F24 to this fact. In such a case the contracting parties will agree a higher liability amount in exchange for the customer's take-over of the costs incurred for a surplus insurance.

8.7 Where the services can only be provided subject to the provision and availability of communication routes by telecommunications services providers, F24 will assume no responsibility for the provision and availability of the communication routes, unless such provision is denied due to the intentional or grossly negligent acting of F24.

8.8 F24 will not be responsible for disturbances affecting facilities, devices and/or implements of communication which were not provided by F24, unless such disturbance was caused intentionally or with gross negligence by F24.

8.9 For claims for reimbursement of expenses and other liability claims against F24 the provisions of this section 9 will be applicable accordingly.

9. Use by Third Parties:

The customer is not allowed to make available the provided service for use by third parties unless with the consent of F24. The contractual relationship does not entitle the customer to make available the services to third parties.

10 Other Covenants:

10.1 Collateral arrangements, supplementing provisions, modifications of and amendments to the contract on services including the specification of services require the written form to be effective. The waiver of the written form requirement must be made in writing as well.

10.2 The customer's general terms and conditions of business will not be applicable, unless such applicability has been expressly confirmed by F24 in writing.

10.3 Upon expiration of the contract F24 will be entitled to either preserve or destroy all the documentation received from the customer, unless mandatory legal regulations provide otherwise.

10.4 Any assignment of rights or transfer of obligations is subject to the prior written consent of the other contracting party. Section 354 a of the HGB *(German Commercial Code)* will not be affected by the above.

10.5 Venue for all disputes under and in connection with the contract on services shall be Munich if the customer is a merchant *(as defined by German law)* or a legal entity under public law, and provided that no other exclusive venue has jurisdiction pursuant to German law.

10.6 German law shall govern all the legal issues resulting under the services agreement and from its discharge, excluding the application of the United Nations Convention on Contracts for the International Sale of Goods.

Data processing agreement according to Art. 28 EU-GDPR for FACT24 services

FACT24
Crisis Management and Emergency Notification

Between

……..
Company name

Controller

……..

……..
Postal adress

represented by

……..
Mr. / Mrs. Full name

……..
Position

and

F24 AG

Processor

Ridlerstraße 57
D-80339 Munich

represented by

……..
Mr. / Mrs. Full name

……..
Position

The following data processing agreement pursuant to Article 28 (3) and other provisions of Regulation 2016/79 EU (EU General Data Protection Regulation – in brief: GDPR) as well as further applicable data protection provisions shall be concluded as follows:

§ 1 Subject and duration of the contract, content of the order

1. Content

The contractor (processor) processes personal data on behalf of the controller. This contract covers all issues with regard to data protection between controller and processor.

2. Subject matter

The subject matter of the order is described in the existing performance agreement (optional, date: ……) between controller and processor regarding the providing of FACT24 software services to which reference is made here (hereinafter ‚performance agreement').

3. Duration

The duration of this agreement corresponds to the duration of the performance agreement.

4. Nature and purpose of the intended data processing

The nature and purpose of the processing of personal data by the processor for the controller are specifically described in the FACT24 performance agreement according to § 1 (2).

F24 develops and operates highly secure telecommunications solutions for providing alerts and communications in emergencies and crisis situations. Using the FACT24 alert and crisis management service, F24 customers automatically alert their management crisis teams in the case of an emergency, can initiate ad hoc conference calls with the push of a button or activate an info hotline on short notice. Using the integrated secure messenger TrustCase, customers can send alerts and work together in virtual crisis rooms.

In this context, specialists at F24 analyse the customer's communications needs when an event happens and support their users when mapping potential scenarios or provide assistance during implementation when using FACT24 or provide customer support.

Data is collected, processed and used within the scope of fulfilling the purposes described above, so long as a contractual relationship is in place for the use of the FACT24 service.

Processing data within the context of the FACT24 process is intended to avoid or minimise material and/or non-material damages to persons and things as part of an incident and crisis management service. The purpose of the FACT24 process is not to evaluate the personality of persons included in the process.

5. Location of data processing

The provision of contractually agreed data processing tasks may only take place within a member state of the European Union or within a contracting state to the Agreement on the European Economic Area or within a state, which has been recognised as providing an adequate level of data protection. Any transfer of data / data processing activities to third countries requires the controller's prior consent and may only take place if the specific terms of Art. 44 GDPR are met.

6. Type of data

The type of personal data is specifically described in appendix 1, procedural notice FACT24:

- *Master data of FACT24-Users*
- *Master and further qualifying data of the persons that shall be notified via FACT24 alerting services*
- *Communication and contact data of users and persons (e.g. telephone, email,…)*
- *FACT24 user's support-requests*

No data within the meaning of Article 9 GDPR is stored or processed as part of the FACT24 process.

7. Categories of data subjects

The categories of persons affected by the processing (data subjects) particularly relates to:

- *Employees*
- *Point of contacts from external organisations (e.g. customers, suppliers, business partners, authorities' contact persons)*

§ 2 Controller's obligations / right to control

1. In the context of the contractual relationship between controller and processor, the controller is responsible for assessing the legal admissibility of the processing to be performed by the processor with regard to GDPR provisions and other rules on data protection.

2. The controller has the right to carry out inspections in consultation with the processor or to have them carried out by an examiner to be named on a case-by-case basis. The controller moreover has the right to verify that the processor complies with this agreement in his business. The execution of such random checks shall be announced on reasonable notice.

3. The processor shall ensure that the controller can convince himself of the processor´s compliance with regard to all of the latter´s obligations in accordance with Art. 28 GDPR.

   Upon request, the processor undertakes to provide the controller with all necessary information, what particularly applies to evidence on the implementation of appropriate technical and organisational measures and obligations agreed upon in this agreement by suitable means.

   The demonstration of such measures, which do not only concern the concrete order/agreement, is feasible in any of the following ways:

- *Compliance with a code of conduct in accordance with Art. 40 GDPR*
- *Certification according to an approved certification procedure in accordance with Art. 42 GDPR*
- *Current certificates, reports or statements issued by independent bodies (e.g. privacy or auditors, accountants, data protection officers, IT security department)*
- *Appropriate certification through IT-security or privacy audits such as e.g. ISO 27001*

Processing of data in private homes shall be agreed on as admissible. In such cases, the processor has to ensure that any applicable data protection provision is observed.

4. The processor is obliged to inform the controller immediately if the processor finds any errors or irregularities especially regarding data protection regulations in the context of the examination of order results.

§ 3 Processor's obligations

In addition to compliance with the provisions of this agreement, the contractor has to comply with statutory obligations set forth in Art. 28 to 33 EU-GDPR. In particular, the processor has to make sure his compliance with the following issues:

1. Written appointment of a data protection officer (DPO), if required by law. Atarax GmbH & Co. KG has been appointed as processor's data protection officer, Email: dataprotection@f24.com. Any changes with regard to the appointment of a DPO and the latter´s contact details must be communicated immediately to the controller.

2. Confidentiality pursuant to Art. 28 para. 2 lit. b, 29, 32 IV GDPR is guaranteed. The processor will only employ and use staff and subcontractors that have been made aware of all relevant data protection regulations; Moreover, the processor confirms that any staff has been obliged to maintain confidentiality in written. Such obligation shall be designed to outlast the termination of the agreement. If relevant for this agreement, the processor also undertakes to commit its staff to the following specific confidentiality requirements:

   ……...
   (e.g. banking-, telecommunication-, social secrecy or professional secrets)

3. The processor will, in his sphere of responsibility, design and regularly check internal organisational structures and processes so that these meet the special requirements of data protection and also guarantee the protection of rights of individuals concerned. He undertakes to implement and comply with all technical and organisational measures required for this order in accordance with Art. 28 para. 3 sentence 2 lit. c 32 GDPR [see Appendix 2 for details on technical and organisational measures taken].

   The processor warrants that he fulfils his obligations under Art. 32 para. 1 lit. d GDPR, and to establish a procedure for the periodic review of the effectiveness of technical and organisational measures to safeguard data security.

4. Concerning the performance of their duties under applicable data protection regulations, controller and processor will cooperate upon request of the supervisory authority.

5. Unless the processor is obliged to data processing by European Union law or by local laws to which the processor is subject (e.g. investigations by law enforcement units or authorities), the processor will only processes controller's personal data in accordance with contractually specified conditions and controller's specific individual instructions.

In such a case, the processor shall inform the controller of these legal requirements prior to processing, unless the law prohibits such communication because of an important public interest or further legal reason the processor is obliged to comply with. The processor shall not process data for any other purposes and is not entitled to forward them to third parties.

The processor shall immediately inform the controller if he considers an instruction as violating applicable data protection law. The processor may suspend the execution of the instruction only until it has been confirmed or changed by controller‘s authorized personnel / representatives where the controller shall bear any risk and cost from the execution of any such instruction turning out to be illegal.

6. The processor is obliged to provide the controller with information at any time as far as controller’s data and documents are concerned.

7. The processor keeps records of processing activities in accordance with Art. 30 para. 2 GDPR and makes them available upon controller‘s request. The controller provides the processor with necessary information required for this purpose. The processor moreover supports the controller in preparing the necessary data processing record required under Art. 30 para. 1 GDPR.

8. The processor shall assist the controller in complying with any obligation set forth in Art. 32 to 36 GDPR. These include:

   a. ensuring an adequate level of data protection through technical and organisational measures that take into account circumstances and purposes of processing activities as well as the predicted likelihood and severity of potential infringements of a data subject´s rights caused by security deficiency and enable immediate detection of relevant injuries and incidents,
   b. the obligation to immediately report data breaches to the controller, usually within 24 hours,
   c. the obligation to assist the controller in the context of the latter´s obligation to inform data subjects, and to provide him with all relevant information without unduly delay,
   d. supporting the controller in the framework of privacy impact assessments,
   e. supporting the controller in the framework of consultations with the supervisory authority.

   The processor may seek compensation for any supportive action he performs in favor of the controller if such action is not part of the contractual duties of the processor and when such action does not have to be performed as consequence of any misbehavior of the processor in regard of this contract.

9. The processor must inform the controller immediately about any actions and measures of supervisory authorities, as far as such relate to this order. This also applies in case that a competent authority initiates any administrative or criminal proceedings against the processor in regard of any data processing activities carried out by the processor.

   In the event that the controller is subject to an inspection by the supervisory authority, an administrative offense or criminal procedure, claims of data subjects or third parties or any other claims in the context of data processing activities in cooperation with the processor, the processor shall support the controller to the best of his ability.

§ 4 Return and deletion

Copies or duplicates of data must not be created without controller‘s knowledge. This does not include backup copies, to the extent necessary to ensure proper data processing, and copies required to comply with legal retention periods.

Data included within the FACT24 process is fundamentally input and erased by the data controller. Six months following the elimination of the purpose set out under no. 4, F24 independently erases customer data, without requiring further approval of the controller. During the term of the contract, log files from alert cases (alarm logs) are available for a period of two years for download by the client and are erased following this period.

The processor must keep documentation that provides relevant evidence of orderly and proper data processing in accordance with respective retention periods even beyond the end of this agreement. In order to discharge himself, the processor may hand over such documents to the controller upon termination of this agreement.

§ 5 Subcontractual relations

1. The processor may only employ subcontractors (other processors) provided the controller´s prior consent is given.

   The controller agrees to employ the subcontractors listed in Appendix 3, provided a contractual agreement in accordance with Art. 28 para. 2 to 4, 9 EU-GDPR exists, either in writing or in a legally admissible electronic format.

2. Prior to employing further or replacing existing subcontractors listed in this agreement, the processor shall inform the controller in due time, either in writing or in text form.

3. The controller may - for important data protection reasons - object to such changes within a reasonable period of time (no longer than two weeks) and appeal to the address/body the processor specified. If there is no objection within the deadline, acceptance of change is considered given. It shall be understood and agreed that any limitation of the service owed from this contract that results from any unfounded objection shall not be part of the responsibility of the processor.

   If important data protection reasons justify the controller’s objection to a specific subcontractor and if a mutually agreed solution between the contracting parties is not to be reached in other ways due to important data protection reasons, the processor shall be entitled to an exceptional right to termination of this agreement.

   In exceptional cases an agreement in the aftermath shall be possible. The processor then shall immediately inform the controller about the exchange of a subcontractor.

4. Subcontracting in the sense of this agreement always refers to services that directly relate to the provision of the main service, i.e. FACT24. This does not include other ancillary services provided by the processor, such as marketing, contract management, billing, invoicing and telecommunications services, postal / transport services or the disposal of data carriers and other measures with the aim to ensure confidentiality, availability, integrity and resilience of hard- and software of data processing systems

However, the processor shall be obliged to hold appropriate and legally compliant contractual agreements and control measures for outsourced ancillary services in order to guaranteeing data protection and data security of controller‘s data.

§ 6 Instructions

Data processing is carried out exclusively within the framework of the agreements made and according to controller instructions. The controller shall generally issue all instructions and orders in writing or in a documented electronic format. Within the framework of the order description made in this agreement, the controller reserves a wide-ranging right to instructions regarding type, scope and procedure of data processing, which may be substantiated by means of individual/detailed instructions.

Changes to the subject matter of this agreement as well as procedural changes must be jointly agreed and documented in written or electronic form. The controller has to confirm verbal instructions immediately in writing or in a documented electronic format.

The performance agreement lists the individuals that are entitled to issue instructions on behalf of the controller as well as the individuals are entitled to receive instructions on behalf of the processor.

In the event of a change or long-term absence of the contact person, the respective contracting party has to be notified immediately in written or electronic form about the deputy or successor.

Controller instructions are exclusively issued by responsible staff members in charge of the relevant subject group named in the performance agreement.

§ 7 Rights of data subjects

1. The processor may not correct, delete or restrict the processing of the data processed on behalf of the controller unless a corresponding and documented instruction has been issued by the controller. In the event that a data subject directly addresses the processor in this regard, the processor must immediately forward such request to the controller.

2. The processor will not be held liable in cases where the data subject’s request is not answered, is not answered correctly, or is not answered in time by the controller, as long as the processor has fulfilled its obligations relating to data protection.

§ 8 Confidentiality

1. The contracting parties undertake to keep the information made available to each other under this agreement as well as any knowledge they obtain from the other contracting party under this cooperation be it on technical, commercial or organisational matters confidential and not to use or make available such information to third parties for the duration or after the termination of this agreement without prior written consent of the other party. The use of any such information or knowledge is limited to the fulfilment of this agreement.
2. This confidentiality obligation does not apply to information

   – *that had already been generally known upon conclusion of the agreement or*
   – *that subsequently became generally known without any breach of a provision contained in this agreement.*

3. The contracting parties shall also impose these data protection and confidentiality obligations to any individuals and companies they employ in the context of this cooperation.

§ 9 Technical and organisational measures

1. The technical and organisational measures described in Appendix 2 shall be defined as binding.

   The processor must ensure security according to Art. 28 para. 3 lit. c, 32 GDPR, in particular in connection with Art. 5 para. 1, 2 GDPR. In general, the actions to be taken consist of data security measures and measures that shall guarantee a level of protection commensurate with the risk as regards confidentiality, integrity, availability and resilience of systems. In this regard, state-of-the-art technology, implementation costs and the nature, scope and purpose of the processing as well as the varying likelihood and severity of risk for rights and freedoms of individuals within the meaning of Art. 32 para. 1 GDPR shall be considered.

2. Technical and organisational measures are subject to technical progress and further development. In that regard, the processor shall be allowed to implement alternative adequate measures. In doing so, the safety level shall be equivalent to specified measures. Significant changes shall be documented.

   As far as the security measures taken by the processor do not meet controller's requirements, he shall inform the controller immediately. The same shall apply to any disturbance, that relate to the data processing.

§ 10 Liability

Existing statutory regulations apply for any liability caused by both, violations of privacy provisions of this agreement or of applicable data protection laws and regulations.

§ 11 Miscellaneous

1. Changes and amendments to this agreement and all of its components - including potential assurance provided by the processor - shall be made either in writing or in an electronic format (text form), including an explicit note on the fact that an amendment or addition is intended. This also applies to the waiver of this form requirement.

2. The processor's statutory seat shall be the place of jurisdiction for both parties.

3. Should individual parts of this agreement be ineffective, this does not affect the validity of the agreement as such. The parties shall replace the ineffective provision by a valid provision of the content closest possible to the initial economic intent of the parties.

……, the ……

On behalf of the controller:

Full name	Signature

On behalf of the processor:

Full name	Signature

Appendices

1) FACT24 Procedural notification
2) Technical and organisational measures (TOM) persuant to Art. 32 EU-GDPR
3) F24 AG subcontractors persuant to Art. 28 (2)-(4) EU-GDPR