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.

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.

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.

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.

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.

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).

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 TEMPLATES

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

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.

OUTBOUND LOCATION-BASED ALERTING

Alert people based on their location.

QUALIFICATION-BASED ALARM GOAL

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

MESSAGE SCOPE

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

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.

INBOUND LOCATION-BASED ALERTING

Trigger the correct alarm depending on the location of the alarm trigger.

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.

ESCALATION

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

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.

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.

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.

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.

ONLINE MONITOR

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

ALARM REPORTS

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

STATISTICS

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

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.

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.

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.

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.

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 Description of the primary related data or categories of data	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. 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.

Version: 01/02/2023