Acubiz - Compliance overview

Updated: 04-03-2025

What is Acubiz?

The Acubiz Solution is a web and app based service for managing expenses. It offers an automated workflow for handling electronic transactions and cash expenses, streamlining the creation, approval, and export of travel expense reports for integration into financial management systems. Key features include credit card and travel account integration, cash outlay reimbursement, advance management, daily allowance calculation, and travel order processing.

Available as a hosted SaaS solution, it supports various business sectors, including pharmaceuticals, finance, legal, auditing, and transportation. Visma Acubiz oversees its development and distribution, providing system development, implementation, and support.

Auditor’s reports

Acubiz has an ISAE 3402 type II and ISAE 3000 type II auditor’s report. The latest auditor’s reports are available free of charge on Acubiz’ website here.

License

What are the license conditions for the amount of licensed users?

The license model can be set up according to the following options:

- Payment per user
- Payment per transaction
- Payment per user and transactions in combination
- Fixed licenses

Can our solution be scaled?

The solution is fully scalable in terms of users and transactions.

Is it possible to monitor license usage?

Acubiz continuously monitors license usage.

Hosting

Acubiz is a part of Visma, and all data and all services are hosted by Visma Software International AS (hereafter "Visma IT") in Oslo. Visma IT provides both infrastructure and services for security, monitoring, backup, patching and all other IT related components and services, and holds its own ISAE 3402, ISAE 3000 and ISO 27001 auditor's reports.
No Acubiz employee has direct access to data or servers within the datacenter. It requires 2-factor authentication through Visma IT's VPN and Firewall, and all access to the solution goes through a Cloudflare, Firewall and HAProxy setup.
Acubiz employees do not have physical access to the datacenter itself.

Backup

Is our system backed up?

Yes, the system is backed up daily. See ISAE 3402 (12.3.1).

Is the process for backup automated?

Yes, the process is fully automated. See ISAE 3402 (12.3.1).

Do Acubiz use encryption of data when it is being transferred or at rest?

Our backup data is encrypted at rest and in transfer.

Does Acubiz comply with data protection rules?

Yes, Acubiz complies with the rules for data protection within backup. This is based on compliance with ISO 27001 controls. Our datacenter (who performs the backup) has both an ISAE 3402 and an ISAE 3000 auditor's report.

Is metadata secured?

The metadata is backed up and secured exactly as all other data.

Documentation of Backup processes:

To see our documentation of our backup processes, please see ISAE 3402 (12.3.1).

Where is the data placed?

Our backup data is kept on multiple locations, controlled by the Visma IT hosting center in Oslo.

Is the system backed up before patching?

The system is backed up before patching, so if any unforeseen problems occur then it is possible to restore the system.

Service Maintenance

Is our patching system automated?

Our patching system is automated, which helps us with an easier patching process and minimizing risks of delays.

Is there a test environment before the patches are released?

Yes, we have a test environment to validate the patches that are going to be released, before they are implemented in the production environment.

What is the procedure for reporting of test results?

The results from the test procedure are documented. To read more about this see ISAE 3402 (14.2.9).

How do we communicate with our customers about new patches?

Description of changes and new features for our standard system can be found on our website here.

Who has the responsibility and cost when errors and compatibility problems occur after new patches?

Acubiz is a SaaS (software as a service), which means Acubiz is responsible for operational stability after new releases of our standard solution. Acubiz bears the cost of new standard releases, which is included as part of the subscription payment.

Security & data protection

Is data protected and encrypted by industry standard?

Yes, all data, both in transit and at rest, is fully encrypted by industry standard encryption protocols. Encryption at rest is provided by Visma IT, and all communication from browsers and apps are through https.

Does Acubiz comply with data protection standards?

Acubiz complies with data protection standards, which can be read more about in our Data Processing Agreement (DPA) and ISAE 3000 auditor's report which provides assurance about our data processing in accordance with the DPA. Our datacenter has an ISAE 3000 which also outlines that it complies with the data protection standards.

Data

Is there a Data Processing Agreement between the company and Acubiz?

There is a legally binding agreement that outlines the terms of data processing between your company and Acubiz. This agreement includes, for example, data ownership, distribution of responsibilities, and security measures.

Is there a clear formulated policy on how data is handled?

Acubiz retrieves electronic transactions from data providers on weekdays (Monday to Friday) and uploads these transactions to servers and into the customer's service configuration, provided the customer has selected this service option. Acubiz's responsibility is limited to data transportation, not the content of individual data files. Customers are responsible for any costs incurred from correcting erroneous data files received from their data providers or for adjustments made by Acubiz. Furthermore, customers bear all costs associated with setting up EAN numbers and other tasks related to their data providers. Additionally, Acubiz reserves the right to use customer data in an anonymized form for statistical purposes or to improve user experience, in accordance with the Data Processing Agreement stipulated in the contract.

Is there any safety documentation?

In Acubiz we have an ISAE 3402 which proves our safety measures and an ISAE 3000. Our datacenter has an ISAE 3000, ISAE 3402 and an ISO 27001.

How is the data retention policy?

Our Data Processing Agreement (DPA) is a legally binding document that outlines the terms of data processing between your company and Acubiz. This includes ownership of data, the distribution of responsibilities, and security measures. There is a clearly articulated policy, which describes how data is processed, the types of data collected, and how they are protected.

Has there been done a risk assessment plan and made contingency plans?

In the event of security incidents and breaches, plans have been established for reporting and addressing these issues. This can be seen in the ISAE 3402 (16.1.12).

Have the employees within Acubiz been trained for a potential security breach?

All Acubiz employees receive training for handling potential security breaches, as documented in the ISAE 3402. This can be found in ISAE 3402 (7.2.2).

Has there been made guidelines for user administration?

Our Help Center provides clear guidelines on user administration procedures and a lot of other matters. This specific guideline can be found on our website here.

Service & Support:

How is the support procedure?

The support will be able to help with the following:

a. Instruction and guidance of key administrators who have been trained by an Acubiz consultant.
b. Automatic import of e-transactions
c. Emergency Critical Error corrections to the Service

If the question pertains to the above, the support team will respond back, or they will need to consult with a specialist. In situations involving an 'Emergency critical error' where the support team cannot fix it, it will be necessary to involve a developer. These situations will take longer to resolve, depending on the severity.

How will the support prioritize the request?

We aim to respond to all support inquiries within 24 hours, and in situations where inquiries are made on Friday afternoon, one should expect a response by Monday. Depending on the nature and complexity of the question, they are prioritized accordingly, and whether the necessary personnel are available to assist.

When is it possible to contact the support?

It is possible to contact the support from 9 AM to 4 PM CET (Central European Time).

How can the customer reach the support?

Support can be reached via phone and email. The email to the support is support@acubiz.com and the phone number is +45 70 214 215. It is only possible for Pro users (finance- and administrator users) to contact the support, otherwise it will be invoiced to the customer.

Is there any self-service support?

Yes, we have our Help Center where it is possible to find different guides and videos on how to use the system. The Help Center can be found here.

What tools does the support use?

The support uses the support system developed by Zendesk.

What can the support help with?

The following table outlines what is included in our support services:

Enquiry from end users
● Only enquiries from Pro-users are included in Acubiz support. ● When end users enquire, Acubiz will always refer them to your Pro-user(s).
Guidelines available in the Acubiz Help Center
● Support that can be resolved with a support guide from the Acubiz Help Center is not included in the support agreement. This also applies even if the enquiry comes from a Pro-user. ● Please refer to the Acubiz Help Center.

Third party e-transaction integrations
● If the solution fails due to missing or incorrect data from a third party supplier, Acubiz cannot provide support. Please refer to the data provider.
Help with setup and configuration changes after commissioning (and Pro-user training)
● Pro-users have access to make a number of changes themselves via the administration platform and are instructed in this during Pro-user training. In such cases, support from Acubiz will be invoiced in accordance with the current price list. ● Requests for new configurations or new features that were not part of the original setup will be invoiced according to the current price list.
Other
● Deletion of data according to the erasure procedure, i.e., according to a written deletion request (DPA, Appendix C, C.4). ● Problems with Acubiz platform login due to user error (and not system technical errors).

Documentation

How is the implementation documentation?

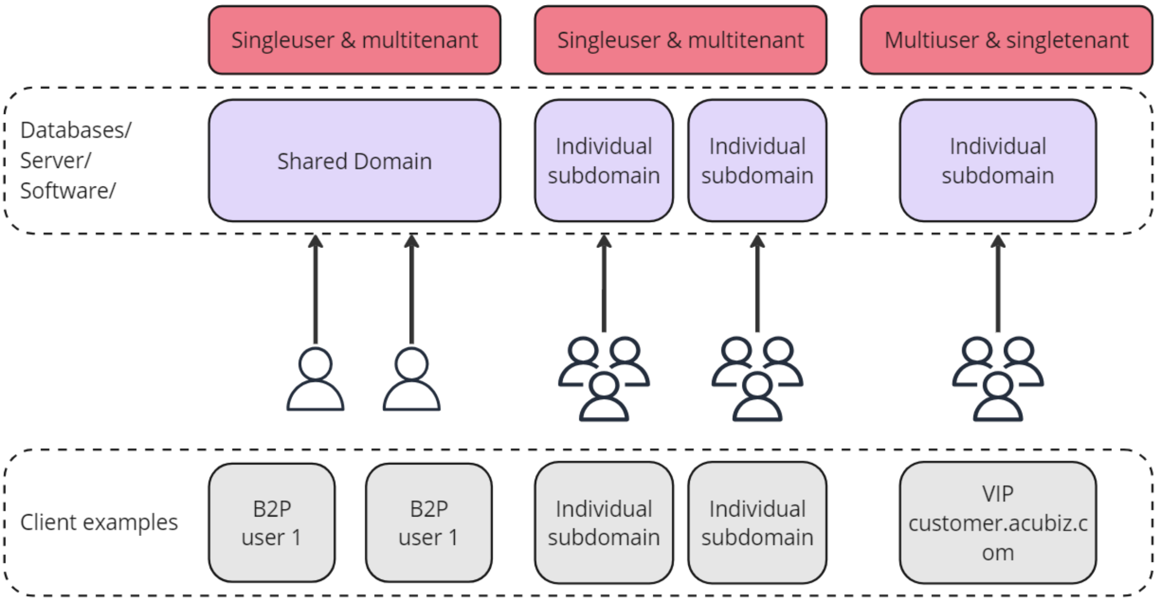
If there are any questions about implementation manuals, technical questions or guidelines for operation and maintenance, then it is possible to find it in our Help Center here.

In the below table it is possible to see how the implementation is done for each stage:

Implementation of Acubiz Service	Performed by	Carried out at
Clarification of Acubiz service	Acubiz	Acubiz
Setup and configuration of standard solution	Acubiz/Customer	Acubiz/Customer
Creation of the first users and action plan	Acubiz/Customer	Acubiz/Customer
Training of superusers	Acubiz	Acubiz/Customer
Ordering of specific apps	Acubiz	Acubiz
Setup of approvers	Acubiz/Customer	Acubiz/Customer
Setup of financial integration	Acubiz/Customer	Customer
Testing	Acubiz/Customer	Customer

Acubiz Infrastructure

In Acubiz it is possible to choose between different hosting/tenant settings. The possibilities can be seen down below:

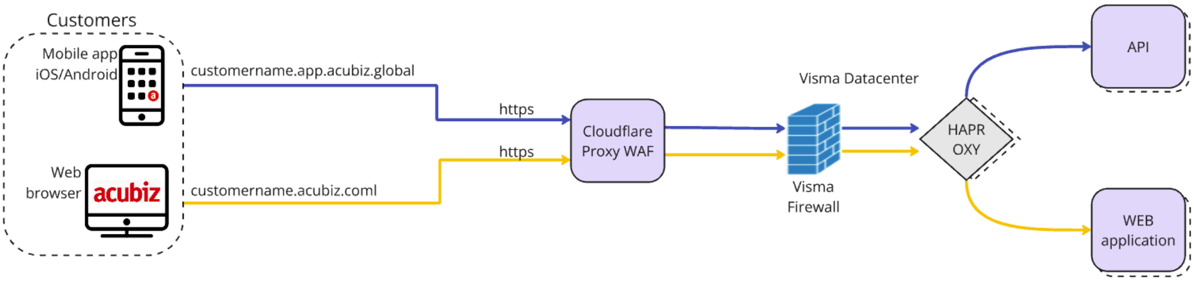


Acubiz offers a SaaS Expense Management solution distributed through a powerful and secure cloud architecture. We have therefore two options for customers:

1. STANDARD SaaS - Shared hosting and shared server in EU/EEA based datacenter. Multiuser/multitenant. For most customers.
2. VIP SaaS - Shared hosting and private server in EU/EEA based datacenter. Multiuser/singletenant. Usually for larger customers who do not want to host the data/application but prefer full separation of data.

Acubiz offers a standard mobile-app for all customers which follows the normal refresh and update cycle for iOS and Android applications.
Utilizing the latest technologies, we proxy all traffic through a Cloudflare web application firewall and every customer has 2 unique hostnames. One for the mobile-app and one for web browsers (usually admin/finance - both can be distributed (https://customername.acubiz.com for the browser and customername.app.acubiz.global for the app)).
For STANDARD and VIP options, Acubiz is utilizing a private cloud setup with Visma Software International AS as hosting partner. The datacenter location is Norway (EU/EEA).

Below it is possible to see how the VIP PLUS Hosting is split up with the other customers:



Acubiz Control Objectives ISAE 3402 type II

5 Information security policies

5.1 Management direction for information security

5.1.1 Policies for information security	Information security policies are established and endorsed by management, then disseminated to employees and relevant external parties. This ensures widespread awareness and adherence to security protocols.	✓
5.1.2 Review of policies for information security	Information security policies are regularly reviewed at predetermined intervals or in response to significant changes, ensuring their ongoing relevance, adequacy, and effectiveness. This process guarantees that the policies remain suitable and effective over time.	✓

6 Organisation of information security

6.1 Organisation of information security

6.1.1 Information security roles and responsibilities	Information security responsibilities are clearly defined and assigned.	✓
6.1.2 Segregation of duties	Duties and responsibilities are segregated to minimize unauthorized or accidental modifications and misuse of organizational assets.	✓
6.1.5 Information security in project management	Information security is integral to project management for all project types.	✓
6.3 Information security awareness, education and training	Management is continuously being trained in awareness and knowledge of new upcoming legislation relevant to the services provided, including NIS2.	✓

7 Human resource security

7.1 Prior to Employment

7.1.1 Screening	Background checks on employment candidates are conducted as per legal, ethical standards, and proportional to business needs and risks.	✓
7.1.2 Terms and conditions of employment	Contractual agreements with employees and contractors specify both parties' information security responsibilities.	✓

7.2 During Employment

7.2.2 Information security awareness, education and training	Employees and relevant contractors receive regular, job-specific training and updates on organizational policies and procedures.	✓

8 Asset management

8.1 Responsibility for assets

8.1.1 Inventory of assets	Information-related assets have been identified and inventoried, with ongoing maintenance of this inventory.	✓
8.1.3 Acceptable use of assets	Rules for the acceptable use of information and related assets have been identified, documented, and implemented	✓

8.2 Information classification

8.2.1 Classification of information	Information must be classified based on legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification.	✓

9 Access control

9.1 Business requirement of access control

9.1.1 Access control policy	An access control policy is established, documented, and regularly reviewed to meet business and information security needs.	✓
9.1.2 Access to networks and network services	Users are granted access only to network and services for which they have specific authorization.	✓

9.2 User Access Management

9.2.1 User registration and de-registration	Formal user registration and de-registration processes are in place for assigning access rights.	✓
9.2.3 Management of privileged access rights	Privileged access rights are strictly allocated and controlled.	✓
9.2.5 Review of user access rights	Asset owners regularly review users' access rights.	✓
9.2.6 Removal or adjustment of	Access rights are removed or adjusted for employees and external users upon employment termination or contract change.	✓

access rights		

11 Physical and environmental security

11.1 Secure Areas

11.1.1 Physical security perimeter	Security perimeters are established to protect areas with sensitive or critical information and processing facilities.	✓
11.1.2 Physical entry controls	Secure areas are guarded by entry controls to allow access only to authorized personnel.	✓
11.1.3 Securing offices, rooms and facilities	Physical security measures are designed and applied for offices, rooms, and facilities.	✓

12 Operations Security

12.1 Operational procedures and responsibilities

12.1.2 Change management	Changes impacting information security have been controlled across organization, processes, and facilities.	✓
12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments have been segregated to minimize unauthorized access or changes to the operational environment.	✓

12.2 Protection from malware

12.2.1 Controls against malware	Detection, prevention, and recovery controls against malware have been implemented alongside user awareness.	✓

12.3 Backup

12.3.1 Information Backup	Backup copies of information, software, and system images have been regularly created and tested according to a predefined backup policy.	✓

12.4 Logging and monitoring

12.4.1 Event logging	Event logs recording user activities, exceptions, faults, and security events are produced, maintained, and reviewed per established documentation.	✓
12.4.2 Protection of log information	Logging facilities and information are safeguarded against tampering and unauthorized access.	✓

12.6 Technical vulnerability management

12.6.1 Management of technical vulnerabilities	Information on technical vulnerabilities is promptly obtained, evaluated for organizational exposure, and addressed with appropriate measures to mitigate associated risks.	✓
12.6.2 Restrictions on software installation	Rules for user software installation have been established and implemented.	✓

13 Communications security

13.1 Network security management

13.1.1 Network security management	Networks are managed and controlled to safeguard information in systems and applications.	✓

14 System acquisition, development and maintenance

14.2 Security in development and support processes

14.2.1 Secure development policy	Established rules for software and system development are applied within the organization.	✓
14.2.2 System change control procedures	Changes within the development lifecycle are controlled using formal change control procedures.	✓
14.2.3 Technical review of applications after operating platform changes	Business-critical applications are reviewed and tested to ensure no adverse impact on organizational operations or security when operating platforms are changed.	✓
14.2.4 Restrictions on changes to software packages	Modifications to software packages are discouraged and limited to necessary changes, with strict control enforced.	✓
14.2.5 Secure system engineering principles	Principles for engineering secure systems are established, documented, maintained, and applied to all information system implementation efforts	✓
14.2.6 Secure development environment	The organization has established and protected secure development environments covering the entire system development lifecycle.	✓
14.2.8 System security testing	Security functionality testing is conducted during development.	✓
14.2.9 System acceptance testing	Acceptance testing programs and criteria are established for new information systems, upgrades, and versions.	✓

15 Supplier relationships

15.2 Supplier service delivery management

15.2.1 Monitoring and review of supplier services	Organizations must regularly monitor, review, and audit supplier service delivery.	✓

16 Information security incident management

16.1 Management of information security incidents and improvements

16.1.1 Responsibilities and procedures	Management responsibilities and procedures are established to ensure a prompt, effective, and organized response to information security incidents.	✓
16.1.2 Reporting and handling information security events and security breach	Information security events must be promptly reported through appropriate management channels. Employees and contractors using the organization's information systems and services should be mandated to note and report any observed or suspected information security weaknesses.	✓
16.1.4 Assessment of and decision on information security events	Information security events are assessed to determine if they are classified as security incidents.	✓

17 Information security aspects of business continuity management

17.1 Information security continuity

17.1.1 Planning information security continuity	The organization has established requirements for information security and continuity management during adverse situations such as crises or disasters.	✓
17.1.2 Implementing information security continuity	A business continuity plan is maintained, reviewed and approved annually. A business impact assessment has been performed to establish the requirements of the business continuity plan.	✓

Acubiz Control Objectives ISAE 3000 type II

Control objective A:

Processing of personal data in accordance with the data processing agreement

A.1 Personal data procedures	Procedures on personal data processing are in place and are assessed regularly as to whether updates are needed.	✓
A.2 Processing of personal data	The data processor only processes personal data in accordance with the instructions given by the data controller.	✓
A.3 Ensuring the processing of personal data in accordance with legislation	Procedures are in place to ensure that the personal data is not processed against the Data Protection Regulation or other legislation. If a case, considered to be against legislation, should arise, the data controller is immediately informed by the data processor.	✓

Control objective B:

Technical measures to safeguard relevant security of processing

B.1 Establishment of security measures	Security measures for the processing of personal data are established and are assessed regularly to ensure that they are up to date.	✓
B.2 Risk assessment and security measures	Up to date risk assessments are made to ensure an appropriate level of security through the implementation of necessary technical measures.	✓
B.3 Antivirus software	Antivirus software has been installed for the systems and databases used in the processing of personal data and are updated regularly.	✓
B.4 Secured access to systems with personal data handling	The external access to systems and databases used in the processing of personal data takes place only through a secured firewall, which has been configured in accordance with relevant internal policy.	✓
B.5 Restricted access to systems with personal data handling	Internal networks have appropriate segmentation ensuring restricted access to systems and databases used to process personal data.	✓
B.6 Restricted users' access to personal data	Users' access to personal data is restricted to a work-related need, which is supported by the agreed technical measures.	✓
B.7 System monitoring and alarm features	Systems and databases used in the processing of personal data have an established system monitoring and alarm feature.	✓
B.8 Encrypted transmission of confidential and sensitive data	The transmission of confidential and sensitive personal data through the internet or by email are protected by effective encryption.	✓

B.9 Protected logon data and logging of user activities	User activities in systems, databases or networks used to process and transmit personal data are logged and reviewed. The logon data is protected against manipulation, deletion and technical errors.	✓
B.10 The use of personal data in development and testing	The use of personal data for development, testing or similar activity only takes place in pseudonymised or anonymised form and is only done according to agreement with the data controller.	✓
B.11 Testing of technical measures	The established technical measures are regularly tested in vulnerability scans and penetration tests.	✓
B.12 Maintenance changes to systems and databases	To ensure maintenance, relevant updates and patches, including security patches, changes are made consistently to systems, databases or networks.	✓
B.13 Granting and removing users' access to personal data	Users' access to personal data is evaluated regularly, ensuring that the granting and removing of users' access is always justified by a work-related need and is removed in a timely manner if no longer found necessary.	✓
B.14 Two-factor-authentication	In the processing of personal data, which involves a high risk for the data subjects, a two-factor-authentification is required for users to access the data.	✓
B.15 Physical access to data centers and premises	Only authorised persons can gain physical access to premises and data centers at which personal data are stored and processed.	✓

Control objective C:

Organisational measures to safeguard relevant security of processing

C.1 Information security policy	A written information security policy, based on the performed risk assessment, is communicated to all relevant stakeholders and is assessed regularly.	✓
C.2 Accordance with data processing agreements	The information security policy generally meets the requirements for security measures and is in alignment with the security of processing in the data processing agreement.	✓
C.3 Screening of employees	As part of the employment process, the data processor's employees are screened for relevant information from their references, criminal record and diplomas.	✓
C.4 Confidentiality agreement	All employees sign a confidentiality agreement and are introduced to the information security policy as well as the procedures for relevant processing of data and other relevant information.	✓
C.5 Deactivation and asset return	Upon resignation or dismissal employees' rights are deactivated or terminated and assets such as access cards and computers etc. are	✓

upon employee resignation or dismissal	returned.	
C.6 Duty of confidentiality after resignation or dismissal	Resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty hereof.	✓
C.7 Security awareness training	Employees regularly complete awareness training on general IT security and security of processing related to personal data.	✓

Control objective D:

Deletion and return of personal data

D.1 Procedures for storing and deleting data	Procedures ensure that the storing and deleting of personal data is made in accordance with the agreement with the data controller.	✓
D.2 Storage periods and deletion routines	Specific requirements for the storage periods and deletion routines of data are in place in accordance with the data processing agreements.	✓
D.3 Termination of data processing	Upon termination of the processing of personal data the data is returned and/or deleted in accordance with the agreement with the data controller and if this is not in conflict with other legislation.	✓

Control objective E:

Storage of personal data

E.1 Storing and processing of data	The processing and storage of personal data follows formalised procedures ensuring accordance with the data processing agreement.	✓
E.2 Localities, countries and regions	The data processing and storage only takes place in the localities, countries or regions that are approved by the data controller.	✓

Control objective F:

Subprocessors adequate security of processing

F.1 Procedures for the use of subprocessors	Procedures for using subprecessors, including requirements for subprocessing agreements and instructions, are in place and are up to date. These are assessed regularly.	✓
F.2 Approving the use of subprocessors	Only subprocessors that have been specifically or generally approved by the data controller are used to process personal data.	✓
F.3 Changes in the subprocessors used	When changing the generally approved subprocessors, the data controller will be informed in time to raise objections and/or withdraw personal data. When changing the specially approved	✓

	subprocessors, this has been approved by the data controller.	
F.4 Data protection obligations	The subprocessors sign a subprocessing agreement subjecting them to the same data protection obligations as those in the data processing agreement with the data controller.	✓
F.5 Required information of subprocessors	The data processor has a complete and updated list of all subprocessors used and approved disclosing: ● Name ● Company registration no. ● Address ● Description of the processing.	✓
F.6 Compliance and risk assessments	Procedures ensure risk assessment of subprocessors and their processing activities as well as compliance with subprocessing agreements.	✓

Control objective G:

Transfer of personal data to third countries

G.1 Accordance with the agreement	Personal data are only transferred to third countries or international organisations in accordance with the agreement and by using a valid basis of transfer.	✓
G.2 Transfer instructions	The data may only be transferred to third countries or international organisations in accordance with instructions given by the data controller.	✓
G.3 Required documentation of a valid basis of transfer	The transfer of personal data to third countries or international organisations is assessed and documented for the existence of a valid basis of transfer by the data processor.	✓

Control objective H:

Handing out, correcting, deleting or restricting information on the processing of personal data to the data subject

H.1 Assistance in the right of data subjects	It is required that the data processor assists the data controller in relation to the rights of data subjects.	✓
H.2 Procedures on data matters	The procedures for timely assisting the data controller include detailed procedures for: ● Handing out data ● Correcting data ● Deleting data ● Restricting the processing of personal data ● Providing information about the processing of personal data to data subjects	✓

Control objective I:

Data breaches responded in accordance with the data processing agreement

I.1 Informed in case of personal data breaches	It is required that the data processor must inform the data controllers in the event of any personal data breaches.	✓
I.2 Identifying personal data breaches	The following controls have been established to identify any personal data breaches: ● Awareness training of employees ● Monitoring of network traffic ● Follow-up on logging of access to personal data	✓
I.3 Time of information of data breaches	In the event of any personal data breach, the data processor must inform the data controller without undue delay and no later than 72 hours after having become aware of the breach.	✓
I.4 Reporting in case of a data breach	In the case of any personal data breach the data processor assist the data controller in filing reports with the Danish Data Protection Agency including detailed descriptions of: ● The nature of the personal data breach ● Probable consequences of the personal data reach ● Measures taken or proposed to be taken to respond to the personal data breach	✓