BEIERHOLM

DECEMBER 2024

IST GROUP AB

ISAE 3000 ASSURANCE REPORT

ORG.NO: 556254-0806

Independent Auditor's ISAE 3000 Report on information security and data protection measures for IST Private Cloud Solution in relation to Data Processor Agreement with Data Controllers.

Beierholm
Approved Accountants
Copenhagen
Knud Højgaards Vej 9
DK-2860 Søborg
Denmark
CVR no. DK 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Structure of the Assurance Report

Chapter 1:
Letter of Representation.

Chapter 2:
Independent Auditor's Assurance Report.

Chapter 3:
Description of the data processing in relation to the IST Private Cloud Solution.

Chapter 4:
Auditor's description of control objectives, security measures, tests, and findings.

CHAPTER 1:

Letter of Representation

IST Group AB processes personal data on behalf of Data Controllers according to signed Data Processor Agreements regarding IST Private Cloud Solution from IST Group AB.

The accompanying description has been prepared for the use of customers and their auditors, who have used the IST Private Cloud Solution from IST Group AB, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the Data Controllers themselves in assessing whether the requirements of the General Data Protection Regulation have been complied with.

IST Group AB hereby confirms that

(A) The accompanying description, Chapter 3, gives a true and fair description of IST Group's data processing related to the IST Private Cloud Solution throughout the period 1 October 2023 – 30 November 2024. The criteria for this assertion are that the following description:

(i) Gives an account of how the controls were designed and implemented, including:

- The types of services delivered, including the type of processed personal data.
- The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase, and limit the processing of personal data.
- The processes utilized to secure that the performed data processing was conducted according to contract, directions, or agreements with the Data Controller.
- The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality.
- The processes securing that - at the Data Controller's discretion - all personal data is erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation.
- The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal data security breaches.
- The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, especially accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored, or processed in other ways.
- Control procedures, which we assume – with reference to the limitations of the IST Privat Cloud Solution – have been implemented by the Data Controllers and which, if necessary, to fulfil the control objectives mentioned in the description, have been identified in the description.
- Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data.

(ii) Includes relevant information about changes in the IST Private Cloud Solution performed in the period 1 October 2023 – 30 November 2024.

(iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the control system that each individual customer may consider important in their own special environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed and worked efficiently throughout the period 1 October 2023 – 30 November 2024. The criteria for this assertion are that:

(i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified,

(ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives, and

(iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 October 2023 – 30 November 2024.

(C) Appropriate technical and organizational security measures are established to honour the agreements with the Data Controllers, generally accepted data processor standards and relevant demands to Data Processors according to the General Data Processing Regulation.

(D) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 3, have been prepared based on compliance with IST Group's standard agreement and related Data Processor Agreement. The criteria for this basis are:

(i) General information security policy
(ii) IT security handbook with reference to the control objectives from ISO27002

Växjö, 2 December 2024
IST Group AB, Ingelstadsvägen 9., SE-352 34 Växjö, Sverige

Mikael Folkesson
Chief Operation Officer

Nikoline Kofod Ravn
Chief Compliance Officer

CHAPTER 2:

Independent Auditor's Assurance Report

For IST Group AB' customers of IST Private Cloud Solution and their auditors

Scope

We have been engaged to report on the description in Chapter 3, which is a description of the data processing in relation to the IST Private Cloud Solution throughout the period 1 October 2023 – 30 November 2024, and on the design and functionality of the controls mentioned in the description.

The report is based on the partial approach, which means this report does not include the IT security controls and control activities related to use of external business partners. These subcontractors are listed in detail in Data Processor Agreements and accompanying appendices.

The reporting engagement does not cover specific circumstances for the individual customer. Furthermore, the report does not cover complementary controls and control activities performed by the Data Controllers.

We express our opinion with reasonable assurance.

IST Group AB's responsibility

IST Group AB is responsible for the preparation of the description in Chapter 3 and accompanying Letter of Representation in Chapter 1, including the completeness, accuracy, and method of presentation of the description and statement, providing the services covered by the description; stating the control objectives; and for designing, implementing and efficiently functioning controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality, and professional conduct.

We apply ISQM 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on IST Group AB's description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3000, Other assurance reports than audit or review of historical financial statements. The standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed and operate effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the data processor's description of the operations of IST Private Cloud Solution, and about the design and operating effectiveness of controls. The procedures selected depend on the judgement of the auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively.

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by IST Group AB in Chapter 3.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at IST Group AB

IST Group AB's description is prepared to meet the common needs of a broad range of Data Controllers and their auditors and may not, therefore, include every aspect of the system that each individual Data Controller may consider important in their own specific environment.

Moreover, because of their nature, controls at a Data Processor may not prevent or detect all data security breaches. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a Data Processor may become inadequate or fail.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description fairly presents IST Private Cloud Solution, such as it was designed and implemented throughout the period 1 October 2023 – 30 November 2024 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 October 2023 – 30 November 2024; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, and the controls had operated effectively throughout the period 1 October 2023 – 30 November 2024.

Description of tests of controls

The specific tested controls and the nature, timing, and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls are solely intended for the Data Controllers, who have used IST Private Cloud Solution and their auditors who have sufficient understanding to consider them along with other information, including information about control measures, which Data Controllers have performed themselves, when assessing compliance with the demands of the General Data Protection Regulation.

Søborg, 2 December 2024

Beierholm
Approved Accountants
CVR-nr. 32 89 54 68

Kim Larsen
Partner, State-Authorized Public Accountant

Jesper Aaskov Pedersen
Director, IT audit

CHAPTER 3:

Description of the data processing in relation to the IST Private Cloud Solution

3. Introduction

The purpose of this description is to provide IST Group AB's customers and their auditors with information regarding the requirements of ISAE 3000, Other assurance reports than audit or review of historical financial statements.

The description is prepared for the use of customers of IST Group AB's joint operations with the other companies of the group – meaning the operations of the consolidated company consisting of the parent company IST Group AB and its subsidiaries IST ApS (DK), IST Sverige AB (SE), IST International Software Technology AS (NO), and IST Deutschland GmbH (DE), which all support the subsidiaries' delivery of products and services aimed at their respective markets. IST Group AB works as sub-processor on behalf of the subsidiaries, who in turn act as data processors in relation to their customers, who are data controllers as defined in the EU General Data Protection Regulation.

The description gives a fair view of the organization, the systems, and the controls for collecting, storing, and other forms of processing personal data in relation to providing IST Private Cloud Solution.

The description is addressing IST Group's customers and their auditors, who have sufficient understanding of roles and responsibilities to consider it together with other information including information about controls performed by the customers, i.e., the data controllers themselves, when assessing compliance with the requirements of the General Data Protection Regulation.

3.1. Description of IST Group AB

IST Group AB was founded in 1982 as a two-person start-up business and has since grown to a consolidated company with 450 employees distributed on 9 offices in subsidiaries in Sweden, Norway, Denmark, and Germany. Since 2015, IST has built up a group structure with common aims, management structure, processes, and business supporting functions.

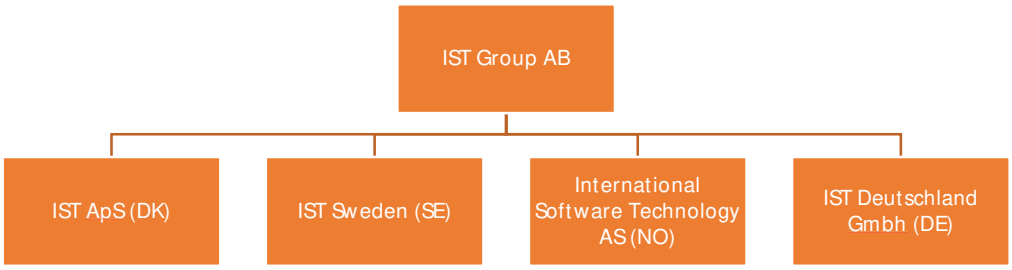

Figure 1 IST Group AB

Figure 2 IST Group AB - Organization

The IST Group provides IT services that support day-care institutions, schools, and youth education programs in public and private sectors at our home markets in Sweden, Denmark Norway, and Germany.

Our solutions include design, development, operations, support, and consultancy services, all with a starting point in digitalizing and IT support of our customers' business areas that are based on legislation within the areas of administration, schools, day-care, youth education etc.
Our close connection with the business areas we are working with ensures that our products and services are developed and adapted in relation to market development, legislation, and the technological development. The layout of our group structure makes it possible for the subsidiaries to act in the local markets as cooperation partners with our customers and to embed knowledge of the domain, demands from customers, and demands from authorities in the development of our products and services.

3.2. Description of data processing

IST Group AB is responsible for providing services to the other companies in the group according to the description below. The services might vary in scope depending on the strategic layout of the individual company within the group.

Furthermore, IST Group AB is responsible for the supporting functions Human Resources, Finance, Business Development, Marketing & Communication, and Corporate IT across the companies of the group.

Service level 1. IST Private Cloud og IaaS

IST Private Cloud includes operation of data centre (IaaS), internal and external networks, perimeter protection, server & storage, database operations, backup/restore, user & rights management, monitoring and 24/7 on-call service. In addition, there is a layer of "Private Cloud Services" including maintenance and operation of: virtualisation environments, container technologies, log handling, performance monitoring.

It is important to point out that when the term "Private Cloud" is used in this description, the meaning is that the business model offers cloud services to the companies within the group. IST Private Cloud is operated on a hardware platform owned 100% by IST. The platform is placed in a "private footprint" in a data centre in Denmark. It means that this is NOT about external organisations buying into IST Private Cloud environments for the purpose of operating their own products and services directed towards their own customer segments.

Service level 2. Operating applications

Operation and maintenance of IST Private Cloud Solution offered to the regional markets are handled by IST Cloud within Tech & Development. The service includes installation and update of services, troubleshooting and corrections, monitoring (on call 24/7), and handling operation-related problems.

Service level 3. Software development and maintenance

The departments Strategy & Vision and Tech & Development in IST Group AB provide production development and maintenance of the solutions SaaS, which the subsidiaries offer on each their markets. The service includes design, development, test, correction of errors, optimization of performance, maintenance, and release of IST's product portfolio.

Although design and development do not necessarily lead to access to customer data, it might, however, result to some extent in processing personal data, for instance error handling, maintenance, test and releases.

Overview of the companies of the group and the services of the IST Group AB:

	IST Private Cloud & IaaS	Application operations	Software Development & maintenance
IST ApS Denmark	Applicable	NOT Applicable	NOT Applicable
IST Sverige AB Sweden	Applicable	Applicable	Applicable
IST International Software Technology AS Norway	Applicable	Applicable	Applicable
IST Deutschland GmbH Germany	Applicable	NOT Applicable	Applicable

In connection with providing these services, IST Group AB must under certain circumstances take on the role as sub-processor on behalf of the subsidiaries of the Group. The division of tasks and the requirements etc. that are subject to data protection rights are laid down in Data Processor Agreements between the companies within the IST Group. The result is that IST Group AB is stated as sub-processor in the Data Processor Agreements between the subsidiaries and their customers (the data controllers).

All such processing of personal data is managed by formally documented policies and procedures. All documents are subject to re-assessment at regular intervals to ensure compliance with relevant legislation.

Processing of personal data can, when subject to certain conditions, be transferred to other sub-processors, who have signed Data Processor Agreement with IST Group AB.

3.3. Personal data

The scope, type, length etc. of the data processing are defined in the Data Processor Agreements and reflect the service level between the different companies. Depending on the relevant Data Processor Agreement, the data processing can include general personal data, confidential information, and in some cases, additional categories of personal data.

The categories of data subjects, included in the data processing, vary according to the agreement with the data controller as well as with the type of service in question.

IST Group AB and its subsidiaries have assessed that scope, type, and length of processing of personal data performed on behalf of the data controllers will, inevitably, imply a high risk for the data subjects' rights and freedom. Add to this issue, the processing of data regarding vulnerable persons (like children, employees), and that the processing includes a really very large number of data subjects as well as during a long period of time. Put together, all these issues will result in demands to a high level of security.

IST Group AB and its subsidiaries (data processors and sub-processors) are on this background allowed to and obliged to make decisions regarding the technical and organizational security measures to implement for the purpose of establishing the necessary (and agreed) level of security.

3.4. Risk assessment

IST Group AB performs and maintains risk assessments of infrastructure, systems, and processes in relation to the specific services provided to the companies within the group.

The risk assessment identifies and exposes the risks related to the data subjects' rights and freedom rights in connection with the processing and includes an assessment of the threats regarding confidentiality, integrity, and availability.

The assessment is the starting point for establishing suitable technical and organizational security measures.

When external service providers are used in the processing of personal data, a separate risk assessment is performed for the services provided by the supplier in question, to support the entire risk assessment and the measures that are initiated to compensate for them.

The risk assessment is performed and maintained by the steering committee for managing information security, and is approved by top management, too.

3.5. Control objectives

To support our role as data processor, IST Group AB has developed and implemented controls to assist us in complying with the General Data Protection Regulation. Below, the introduced procedures and controls are described in more detail.

3.5.1. Control objective A: Instructions regarding processing

Procedures and controls are observed to ensure that the instructions regarding processing personal data are complied with in accordance with the Data Processor Agreement.

According to the internal procedure, a Data Processor Agreement must be signed every time IST Group AB is data processor in relation to other companies with the group. The Data Processor Agreement serves – together with further specific instructions from 1) The companies within the group in their capacity as data processor in relation to 2) The customer, who is data controller – as foundation for the data processing.

All Data Processor Agreements between IST Group AB and its subsidiaries are made with the support from IST Group's compliance department (Standards & Governance). The department performs an assessment of the quality of the agreements, compared with the actual services, as well with as with the legality of the instructions regarding the processing activities connected to the agreement.

According to regular intervals, and in connection with major planned changes in the organization and/or the services between IST Group AB and its subsidiaries, IST Group's compliance department oversees the consistence between the actual processing activities, the Data Processor Agreements, and the instructions.

3.5.2. Control objective B: Technical security measures

Procedures and controls are complied with to secure that the data processor has implemented technical measures to ensure relevant security in the data processing.

IST Group AB has information security as an overall strategic initiative, to which is implemented an information security management system based on the ISO27001 framework. The organization - that takes care of operations and maintenance of IST Private Cloud and Infrastructure-as-a-Service (IaaS) – is included in the present ISO certification and has been included since 2015. In addition, IST's management system is certified for quality (ISO 9001) and environment (ISO 14001).

The management system includes procedures for managing information security, objectives & follow-up, internal & external audits, management's review, systematic improvements, and deviation management. The annual external follow-up audits and 3-year re-certifications are performed by an independent third party (DNV; www.dnv.com) and ensure the efficiency and conformity of the management system in accordance with the ISO standards (27001, 9001, 14001).

The outcome of audits, reviews, and the efficiency of the management system is presented and evaluated by Management at regular intervals, and it is assessed whether our compliance with standards and the data protection legislation is appropriate.

Via the IT strategy, IST Group AB has chosen ISO27002 as point of departure and has in this way used the ISO methodology for implementing the relevant security measures within the following areas:

- Information security policies
- Organisation of information security
- Human resources security
- Asset management
- Access control
- Encryption
- Physical and environmental security
- Operations security
- Communication security
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance with legal and contractual requirements

Asset management

The group's IT equipment and IT resources are recorded in the group's CMDB (Configuration Management Database). The purpose is to maintain updated databases with relevant data for the group's IT equipment, which is necessary for our production and maintenance of SaaS, Private Cloud, and IaaS.

By recording and updating this information in a" CMDB" (Configuration Management Database), we ensure that we have an accurate survey of our IT equipment and its condition. This enables us to carry out efficient management of our IT environment, including identification of potential problems, planning of maintenance and support, as well as fast reaction in the event of incidents and crashes.

- All units in the production environments are recorded in an CMDB.
- Devices (laptops, mobile devices etc.) are managed by MDM (Mobile Device Management)
- Hardware is phased out in an environmentally responsible fashion.
- Data on hard disks is erased according to the NIST.800-88 standard.

Access control

IST uses a role-based access control of rights to hardware, networks, and services. The employees have personal and unique userIDs and are instructed not to share access with others, as well protect access against unauthorized use. Access to the group's internal network and services takes place via multi-factor authentication.

Granting of access takes place in accordance with the group's business purposes and the classification of the information. Via a role-based approach to access control, we ensure that the employees have only the approvals and privileges that are necessary for performing their work without having unnecessary access to sensitive and confidential information.

Applications for granting access to production resources are approved by the nearest leader and documented for traceability, which ensures a strict control over the access to critical systems and data. Extended access rights, like administrator accounts, are only granted to a limited number of staff, who has a direct responsibility for the operation of SaaS. These privileges are granted to individual accounts and are subject to regular control to ensure security and compliance with guidelines. Access logging is performed and is stored for 6 months.

Encryption

Encryption is an important security measure used for protection of data during transportation and storing. Using secure encryption algorithms is decisive for maintenance of high security regarding data communication and storing. Usually, we use TLS (Transport Layer Security) version 1.2 or newer.

- Ensure network traffic between the user's client (browser) and IST's services. HTTPS traffic is filtered through a firewall and redirected to central "load balancers."
- VPN (Virtual Private Network) tunnels are used to ensure the network traffic between customers, third parties, and IST's network.
- SFTP (Secure File transport Protocol) is used for exchanging files between customers, third parties, and IST.
- Secure mail, default setting is set up to use encryption for sending/receiving e-mail via SMTP.
- SSH (Secure Shell) is used to connect to internal networks and servers.
- Backup of files and databases is performed locally and is secured using TLS 1.2 encryption.
- Storage disks (SAN) use encryption for disks that are actively registered in the SAN cluster. When a disk is removed, the encryption is automatically erased within short time.

Physical security

For all offices and buildings, where IST has office premises, there is an established access control (personal tags/pin) and alarm systems with monitoring outside of opening hours. IT equipment is as far as possible locked up and/or ensured by fastening into construction material. Movable devices are either under personal surveillance or locked up.

For data centres there is established physical security as well as 24/7/365 monitoring and several layers of access control. The demands correspond to "Uptime Institute's" TIER 3 classification, which includes that a data centre can be maintained simultaneously with redundant components using redundant distribution channels to service the critical environment. Contrary to the demands of Tier I and Tier II, these facilities require no closing down, when the equipment is maintained or changed. The components in Tier III are added to the Tier II-components meaning that each part can be closed without impacting the IT operation. The components include:

- Units for power, cooling, monitoring
- Redundant power lines and production units (public electricity suppliers, generators).
- 1+N capacity in all critical units.
- Water and fire detection and fighting.
- Systematic test of all units, annual full-scale test of power outage for the entire building.

Operations security

IST Group AB has implemented procedures for work routines everywhere in the organisation. The procedures are owned by each head of department, who is responsible for the procedures being updated, efficient, and communicated to all relevant employees. The steering committee for information security and data protection is responsible for overseeing that the procedures are kept updated and that contact points between process areas work to the best possible effect.

- Operational Change Management Process (OCP)
- Operational Incident Management Process (OIP)
- Software Development Process
- Software Support Process
- Software Release Process

In addition, there is a series of procedure descriptions laying down specific work routines for important and critical operations regarding operation and maintenance tasks.

Supervisory monitoring of operations and capacity is established on production environments and infrastructure. Furthermore, we have 24/7/365 "On-Call" service with staff conducting monitoring and first-line support outside normal working hours. Critical suppliers (data centre, internet-line operator etc.) also use the staff member, who is "On-call" duty as point of contact for critical errors in their deliveries.

The automated monitoring of resources in relation to hardware/data lines etc. is performed via a considerable number of parameters collected as data points in a central database. On this basis, development in load over time can be documented and followed up. The operating staff inspects daily that the load is within the tolerances and times specified.

Backup

Security backup is performed of databases, virtual servers (snapshots), log archives, and binary code libraries to make recovery possible in case of an emergency. Security copies are encrypted and are stored locally in the operations environment. From here, they are transferred to a secondary location via an encrypted data line. There are different requirements to the intervals of security copying, recovery test, storage period, and time for regeneration depending on the importance of the IT services as defined in a security copying policy. At regular intervals, recovery tests are performed to ensure the integrity of the data copied according to security policy.

The requirements to security copying, erasure, and recovery test of customer data are defined in Data Processor Agreements and contracts with customers.

Vulnerabilities, patch, and security configurations

The organisation monitors the development in release of known vulnerabilities in products and services, and the organization has a risk-based approach to this. Operating systems and services exposed to public networks have the highest priority, next on the list is other critical infrastructure.

Procedures for evaluating new known vulnerabilities are established, and likewise how to handle them. Furthermore, system support is implemented for identification of vulnerabilities in third-party libraries used in IST's services.

Work routines are established with requirements regarding the allowed patch level and versions of the operating systems, virtual environments including container, as well as allowed security settings. Only employees with extended access rights can install and update software on equipment in production environments.

Penetration test

At regular intervals various tests are performed of operating environment, networks, and perimeter protection to test the efficiency of the implemented measures. Test can be performed by IST Group's own staff or by external consultants after preceding description of the task and "the Rules of engagement". Test reports are evaluated by operations manager and the steering committee of information security, and any improvements are also decided here.

Cyber threats

Use of services for identification and fighting virus, malware, and other cyber threats are implemented, where it is necessary and based on a risk-based approach. Any exceptions must be approved by management, documented via risk assessment and other established technical measures. The following technical measures are implemented:

- Ddos protection of external data lines towards the internet
- Antivirus and Malware protection on all laptops
- Malware/spam detection in e-mails and other cooperation platforms
- Antivirus on exposed servers based on a risk assessment
- Scanning endpoint for open protocols and known vulnerabilities

Logging

Logging is a useful tool that serves several purposes like monitoring, performance, errors, and is implemented on many levels in the production environment. Logs contain important information about incidents in the systems and users' dealings with data. Logging includes network traffic, connection between services, operator access and system access, occurrence of errors, security logs, application users' system login, and audit trails for users' handling of confidential information etc.

Logs are stored in specific systems and databases suitable for handling large amounts of data in searchable formats and are protected by restricted access on networks and user roles. There are established routines for how long logs on different levels are stored and erased. In addition, when it is necessary, to secure logs against unjustified changes and manipulation.

Communication security (network security)

The connection between production environments, IST's internal network, public communication network (the internet) takes place via two independent data lines with endpoint protection in the form of redundant firewall and load balancer.

Firewalls have an in-built hierarchy of rules on protocol and service that ensures that only approved traffic is permitted into specific segments of the network. In addition, network traffic from unsecure IP

segments is barred (geo-fencing). All incoming and outgoing network traffic is monitored and logged in central services.

The internal networks behind the firewall are divided into several IP segments based on types of service. This is, inter alia, DMZ-zones, infrastructure and operations, service net, database net etc. Access between internal networks is allowed based on protocols and types of services governed by firewall rules.

Segregation of networks is established between production environments, pre-production environments and test environments.

IST's other internal networks for administrative tasks, and available for all IST employees, have no access to production environments.

All transfer of data to third parties and locations outside IST's controlled networks is conducted via encrypted data lines.

Use of remote workplaces/ home office (teleworking)

A possibility is established that enables employees and consultants at IST Group AB to enter internal networks and services from remote workplaces or home offices via external communication lines. There are established measures like encryption, VPN, and multifactor validation to ensure that no unauthorized person can access sensitive and confidential personal information. Any processing performed by employees/consultants is only allowed by using approved units from the workplace.
Operational staff and other employees with work-related needs for access to production networks (IST Private Cloud and IaaS environments) must go through additional multifactor authentication mechanisms before they can access production networks and services.

Use of environments for development, test, and production

Different types of environments are established to use for tasks regarding design, development, test, and correction of errors. Artificial data is used in environments for development, test, and demo. Rules and procedures describe requirements to production data (personally identifiable information). When personal data is processed in relation to identification of errors and verification of correction of errors in production-like environments, there are the same requirements to technical and organizational measures as there are in relation to real production environments.

There are established procedures for software development, support, and maintenance implying that security routines are included in the work of everybody involved in development and operations of our programs and services:

- Software test, including controlling vulnerabilities in third-party libraries.
- Version management and backup.
- Configuration management and backup.
- Automated build and deployment.

Supplier relationships

IST Group has established policies for managing critical suppliers – "Supplier Code of Conduct". Demands regarding information security and data protection are made to suppliers/business partners, who take part in operation and maintenance of IST Private Cloud and IaaS. Risk assessments are performed in relation to supplier and type of cooperation, and service contracts, NDA etc. are signed.

The steering committee for information security is responsible for inspection at regular intervals of suppliers' compliance with contracts and security demands.

Information security incidents management

The organization has implemented procedures for managing information security incidents and data protection incidents – procedures describing work routines, roles, and responsibility for correct and thorough handling. The process is monitored by IST's compliance department that is actively involved in relation to high level or critical incidents and is responsible for involving the organisation's Data Protection Officer when necessary and required. In addition, the efficiency of the process is evaluated in our Management's annual review. Employees performing an active role in the processes receive training and sparring in relation to their role to ensure the necessary quality in this work. All incidents are logged and documented, and information is forwarded to third parties (customers, partners, authorities) when necessary to comply with legislation, directions, and contracts.

Information security aspects of business continuity management

The organisation's total operation structure is composed with a redundant set-up consisting of several layers – when possible and financially profitable. This ensures a relatively high uptime, and we honour the applicable demands of the Service Level Agreements.

Regardless of the above, emergency procedures and re-establishing procedures are established to ensure that the organization will act in case of unexpected and sudden incidents of some size.

Contingency plans are prepared (as business continuity), including description of roles and responsibilities for crisis management, summons, declaration of crisis level, escalation etc. In the event of a major crisis, a Crisis Management Staff is summoned, consisting of members of: Senior Management, Operations and Development, Compliance and Communication. The Crisis Management Staff's purpose is to ensure the best possible framework for re-establishing the operations of the organization.

In the contingency plans there is a description of certain critical scenarios as well as a procedure to counter them. The scenarios are partly based on risk assessments and partly on actual incidents (or near-incidents) and are enhanced on an ongoing basis.

Annual tests are conducted of various parts of the contingency plan. These tests are evaluated and subsequently improvement initiatives are identified.

3.5.3. Control objective C: Organisational security measures

Procedures and controls are complied with to secure that the data processors have implemented organizational measures to ensure suitable security of processing.

The General Data Protection Regulation specifies that suitable technical and organizational security measures must be established. IST Group AB manages this security setup using implemented policies, like policies for:

- Information security management
- Logical access control
- Physical security
- Mobile devices and teleworking
- Classification of information
- Processing/storing/erasing of personal data
- Data breaches

These policies set the general conditions for preventing accidental or illegal destruction, loss, or change, as well as preventing non-authorized transfer of or access to personal data.

In addition to the general polices, a set of procedures is implemented which relates specifically to processing personal data and how to act in compliance with the General Data Protection Regulation.

Information and directions regarding collecting, storing and other kinds of processing personal data are available for all employees on our intranet. All employees receive mandatory training about data protection, and ongoing awareness campaigns are part of our annual plan in relation to security communication.

Organisation of information security

We have established a dedicated steering committee for information security and data protection. The steering committee is responsible for the overall management and control of security & data protection in relation to all IST's products and services we provide to our customers (data controllers).

This steering committee consists of relevant roles from product development, management, and compliance, who are responsible for procedures and work routines in the departments for design, development, and operations.

The steering committee operates in relation to a structured annual cycle of work ensuring follow-up on all aspects of information security and data protection. This includes updating risk assessments, evaluation of security and data protecting incidents, as well as updating and implementing of policies and work procedures.

The committee's primary task is to secure that all relevant security and data protection measures are established and are complied with during all phases of the products' life cycle. The committee identifies and prioritizes risks, defines policies and procedures, and ensures that all employees have the necessary knowledge and training to efficiently handle information security and data protection.

Human resources security

IST upholds severe recruitment procedures to ensure that staff with appropriate competences is employed. Verification is carried out of the applicant's competences, CV, and previous work experience. IST employees are matched against a predefined set of job descriptions that outlines competences, areas of responsibility, place in the organization's structure, and reference to a manager. Obligations in relation to confidentiality, NDA, and code of conduct are a part of the employment contract between IST and the employee.

Onboarding programs are implemented focusing on rules and areas of responsibilities when employed by IST in general – and directions in force at the department in question.
Termination of employment follows the offboarding procedure to ensure that all necessary steps are performed correctly by managers, HR, and Corporate IT.

In the event of purchase of consultancy services or commencing cooperation with third parties in connection with projects, and when confidential information is shared, obligations regarding confidentiality, NDA, and code of conduct are part of our standardized basis of contracts.

IST invests in staff training to secure that all employees and consultants know and understand policies and procedures regarding information security and data protection. We offer regular training programs focusing on the specific directions and best practices applying to our organization.

Data Protection Officer (DPO)

Based on GDPR Article 38, guidance notes from national data protection agencies, and EDPB's (the Article 29 Group's) recommendations in WP 243 rev. 02 – IST Group AB has assessed the need of attaching a data protection officer to our organization. The assessment resulted in establishing a cooperation with an external law firm - Focus Advokater P/S – and from this firm we have appointed Jesper Løffler Nielsen, Associated Partner, Barrister (High Court), PhD as data protection officer for IST Group AB and the other companies in our group.

3.5.4. Control objective D: The right to erasure ("The right to be forgotten")

Procedures and controls are complied with to ensure that personal data can be erased or returned if an agreement is made with the data controller to this effect. The overall division of tasks for managing the individual's rights (including insight, correction, and erasure) between data controller, data processor, and sub-processor is defined in a series of data processor agreements between the parties.

At IST Group AB and the other companies in the group, the allocation of responsibilities is made more explicit in data processor agreements, rules, and procedures to the total effect that IST assists the data controller in conforming to the data subject's rights.

3.5.5. Control objective E: Sub-processor

IST Group AB has implemented a group policy "Supplier Code of Conduct" describing our expectations and demands to suppliers (including sub-processors) in relation to parameters like human rights, quality, privacy protection, information security, sustainability etc.

In addition, a procedure is established about on-boarding, managing, and off-boarding suppliers. The procedure defines responsibility and roles for managing suppliers, and it ensures that relevant demands to security and quality are accommodated.

These procedures outline how to deal with sub-processors:

- In connection with selecting and commencing cooperation: Contracts, terms & conditions, data processor agreements, risk assessment.
- During ongoing cooperation: Follow-up on compliance, updating risks, problem handling.
- And discontinuation of cooperation: Termination of contracts, erasure/returning of data.

3.5.6. Control objective F: Storing personal data

As part of the total framework for information security, we have defined a security policy in relation to third parties, and according to this policy, IST Group AB is not allowed to cooperate with a supplier, who cannot comply with IST Group's security standard. In addition to this, we have implemented procedures for due diligence, review of suppliers, and risk analysis regarding third parties, so that we ensure that a supplier or other third party, who is going to process personal data on behalf of IST Group AB, has implemented appropriate technical and organizational measures to comply with the General Data Protection Regulation.

Depending on the risk assessment, the assessment might be repeated with regular intervals. Furthermore, IST Group AB and the external data processor must sign a data processor agreement, and in this agreement IST Group AB must specify our requirements to securing compliance with the General Data Protection Regulation. The data processor agreement includes a condition stating that IST Group AB can terminate the agreement, in the event the sub-processor does not comply with contractual requirements or does not comply with the General Data Protection Regulation.

According to the data processor agreements between IST Group AB and the other companies of the group, planned changes regarding sub-processors must be communicated well in advance to the companies in the group. Furthermore, it must be ensured that specific demands regarding transfers to third countries and other demands to technical and organizational measures are not impaired in any material way compared to the signed data processor agreements between IST Group AB and the other companies of the group.

3.5.7. Control objective G: Transfer of personal data to third countries

Transfer of personal data to third country or to organizations that have been a hot topic among the public from the summer of 2020. IST Group AB and the regional companies are monitoring the development very closely, and we acknowledge that our governmental customers are very preoccupied with insuring themselves against undocumented transfers to third countries, and all things considered want to totally avoid these issues. Thus, IST's strategy is to try to completely avoid transfers to third countries when possible.

In connection with IST Group AB and the other group companies' customer-facing SaaS solutions, IST Group AB solely transfers personal information to third countries or international organisations, if an agreement has been signed with a data processor or data controller about this by way of a data processor agreement with accompanying specific instructions. In addition, the transfer must be in compliance with GDPR and national legislation regarding transfers to third countries.

When using sub-processors outside EU/EEA boundaries, the requirements for this purpose are defined in IST's Supplier Management Model. In consequence of this, it is, inter alia, stated that all transfers to foreign countries can solely take place on the following background:

- General or specific consent from the data controller/data processor
- Etablishing valid basis of transfer
- Etablishing necessary measures
- Follow-up and control with the transfer

3.5.8. Control objective H: Assisting the data controller

IST Group AB has defined internal procedures and directions for supporting requests from data subjects. This includes descriptions of all necessary steps to reply to such requests, including how the request is processed, who is involved, how to identify a data subject's personal data, and how the process is documented and communicated to the data subject. The procedures support IST Group AB's efforts to comply with the notice of 30 days for replying to a request from a data subject.

In accordance with our procedure, IST Group AB will not accommodate a direct request from a data subject but will always refer to the data controller. The procedure states that information will only be forwarded to the data subject when the data controller has given advance consent in writing.

3.5.9. Control objective I: Data security breaches

Procedures and controls are complied with to ensure that action is taken in relation to every breach on personal data security in accordance with the signed data processor agreement.

IST Group AB has implemented a policy for managing security incidents including information security incidents and/or data protection breaches – a policy stating IST Group AB's general responsibility in the event of security incidents.

In addition to the general policy, IST Group AB has implemented an "Incident Management Process", "Operationel Incident Process", which defines in detail how incidents must be handled including remedial action and reporting to data processor and data controller.

In accordance with the procedure, the data controller must always be informed in case of an incident involving personal data processed by IST Group AB on behalf of the data controller.

3.6. Complementing controls at data processor and data controller

Some of the control objectives included in IST Group's system description can only be fulfilled if action is taken together with complementing and efficiently working controls at data processors and data controllers. The present report does not cover whether such controls have a suitable design, are implemented, or work efficiently.

The Data processor, IST Group AB's subsidiaries (IST ApS, International Software Technology AS, IST Sverige AB and IST Deutschland Gmbh.

It is the data processor's responsibility to have implemented suitable policies and procedures to comply with the requirements of responsibility and obligations laid down in the overall data processor agreement – an agreement containing the following aspect (the list is not complete):

- Personal data forwarded to IST Group AB is updated and correct.
- Securing the legality of the directions forwarded to IST Group AB in relation to data protection legislation in force at the time in question.
- That the directions are in accordance with the data processor agreements and the services provided by IST Group AB.
- That the data processor has appropriate user access management regarding personal data.
- That the role as Incident Manager is described in the procedure for handling data breaches (Incident Management Process), is performed by a competent employee, and is handled efficiently.
- That the procedure for right to insight is handled efficiently in the communication with the data controller and with the data subject, if any.

The data processor IST Group AB are themselves responsible for managing the following control objectives:

- Development, operations, configuration, monitoring, and maintenance of own services provided to IST Group AB's customers.
- Configuration and monitoring of backup.
- Erasure of customer data, database backups
- Handling "the right to be forgotten" in backups.
- Choice of "appropriate security level", re-assessments and follow-ups, and tests of security controls, see Article 32 of GDPR which is relevant for services developed by or on behalf of IST Group AB.
- Keeping records of categories of persons and personal data (Article 30 of GDPR) in relation to proprietary customers services (Article 30 records).

Data controller (customers of IST Group AB's subsidiaries)

- Personal data handed over to IST Group AB's subsidiaries (IST ApS, International Software Technology AS, IST Sverige AB, IST Deutschland Gmbh is updated and correct.
- Securing the legality of instructions transferred to IST Group AB's subsidiaries (IST ApS, International Software Technology AS, IST Sverige AB, IST Deutschland Gmbh) in relation to the data protection legislation in force at the time in question.
- That the user access management to personal data at the data processor is appropriate.

CHAPTER 4:

Control objectives, control activity, tests, and findings

The purpose of this report is to provide information to the data controllers about control measures at IST Group AB that might impact the processing of personal data, and in addition to provide the Data Controllers with information about the operational efficiency of the tested controls.

Below the grey field are three columns:

- The first column tells the activities IST Group AB, according to their documentation, has put into practice to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation, and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation to assess, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at IST Group AB. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control to verify that the control measure works as assumed.

Control objective A: Instructions regarding processing

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistent with the signed data processing agreement.

IST Group's control activity	Beierholm's performed test	Findings
The data processor has procedures for entering into written Data Processor Agreements in accordance with the services provided by the data processor. The data processor uses a standard Data Processor Agreement, when entering into Data Processor Agreements. When entering into written Data Processor Agreements based on the data controller's standard, the data processor uses a check list stating the requirements the data processor must live up to. Data Processor Agreements include information about the use of Sub-processors. Data Processor Agreements must be signed and be stored electronically. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	We have in interviews asked Management about the control measures. Procedures in writing exist including a requirement that personal data must only be processed when a Data Processor Agreement and accompanying instructions to this effect are available. Inspected documentation disclosing the foundation on which personal data is processed (standard for Data Processor Agreement) as well as disclosing that this basis must be approved by the data controller. It is established that a structured work procedure is applied, laying down the demands the data processor must live up to. Inspected that the standard for entering into Data Processor Agreements includes the naming of approved sub-processors. Inspected documentation disclosing that the foundation for processing personal data is based on a signed Data Processor Agreement and that the said agreement is stored in electronic format. We have checked that the procedures are updated.	No comments.
Any signed Data Processor Agreement includes instructions from the data controller. The data processor obtains instructions for processing of personal data from the data controller in connection with signing the Data Processor Agreement. The data processor only processes personal data as stated in the instructions from the data controller.	We have in interviews asked Management about the control measures. Inspected that formalised procedures exist ensuring that personal data is only processed in accordance with instructions. Inspected that the standard for entering into Data processor Agreements includes stating instructions regarding data processing.	No comments.

Control objective B: Technical security measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

IST Group's control activity	Beierholm's performed test	Findings
Risks are minimized based on assessment of their probability, consequences, and derived implementation costs. The findings contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks. Risk assessments are updated on a regular basis as needed, but as a minimum once a year.	Inspected that formalized procedures exist ensuring that the data processor performs a risk assessment to safeguard relevant security. We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly. Inspected that the performed risk assessment is updated and includes the present processing of personal data.	No comments.
pThere is documentation for operational procedures regarding business-critical systems, and the procedures are available to staff with a work-related need. Management has implemented policies and procedures to secure satisfying segregation of functions. A management of the operations environment is established to minimize the risk of technical crashes. An ongoing capacity forecast is performed based on business expectations to growth, and new activities, and the capacity requirements derived thereof.	We have: • Asked Management whether all relevant operational procedures are documented. • In connection with audit of each operational area, controlled via sampling tests that documented procedures are established and that there is accordance between the documentation and the performed procedures. • Performed inspection of users with administrative rights to verify that access is due to work-related needs and does not compromise the segregation of functions. • Asked Management about the performed procedures/control activities. • Reviewed on a sample basis that the resource consumption in the operational environment is monitored and adapted to the expected and necessary capacity requirements.	No comments.
Changes to functionality is tested before they are put into operation. Development and test are performed in development environments that are separated from production environments. A version management system is used to register all changes to the source code.	We have asked Management whether: • An overall quality managing model is devised for handling software development. • Procedures, including accompanying work routines, are in place for rolling out software changes to the live production. • Procedures are in place for separation of the production environment	No comments.

Development environments and test environments are separated from each other.	from the environments for development and maintenance. • Procedures and work routines are in place for dealing with version changes as well as a supporting system for recording changes to the source code. • Formalized procedures are in place for separation of test environments and production environments for use in relation to software development.	
For all systems and databases used for processing personal data, appropriate antivirus systems are installed, and they are updated on an ongoing basis.	We have: • enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks. • enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks. • verified that antivirus software is installed on systems and databases related to IST Private Cloud Solution. • inspected on a sample basis that antivirus software is updated.	No comments.
Backup of systems and databases is performed every day.	We have: • asked Management about the procedures/ control activities performed. • examined backup procedures on a test basis to confirm that these are formally documented. • examined backup log on a test basis to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis. • examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored.	No comments.
For the production environments used for processing personal information, a monitoring system with alarm is established.	Inspected that for systems and databases used for processing personal information, a monitoring system with alarm is established.	No comments.
Especially risky operating systems and network transactions, or network activities are monitored. Deviations are investigated and solved in due time. The systems log when the users log on and of the systems.	We have: • asked Management about the procedures/ control activities performed and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged.	No comments.

Only in the event of suspected or identified abuse of the systems, users are actively monitored. A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur to react proactively.	• checked on a test basis that logs from critical systems are subject to sufficient follow-up. • ensured that a monitoring tool is used and that this is available to all employees. • ensured that alerts are sent by email and SMS, if errors occur.	
Changes to operating systems are carried out according to established procedures which ensure maintenance containing relevant updates and patches, including security patches.	We have asked Management, whether procedures for patch management are established in IST Group AB. By inspection on test basis, we have verified that • adequate procedures are applied, when controlled implementation of changes to the production environment of IST Group AB is performed. • changes to IST Group AB operation environment comply with directions in force, including correct registration and documentation of applications about changes. On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.	No comments.
Networks must be protected against threats in order to secure network-based systems and the transmitted data. Production environment must be secured against failing supply in relation to redundancy to network connection to the internet.	It has been checked that necessary protection against unauthorised access is implemented, including: • Appropriate procedures for managing network equipment are established. • Segregation of user functions is established. • Appropriate logging and monitoring procedures are established. • Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level.	No comments.
Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented. In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.	We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented. We have by inspection on a test basis ensured • that appropriate framework for managing cyber-attacks is devised. • that plans for managing the threat are devised and implemented.	No comments.

	• that the plans include cross-organisational collaboration between internal groups.	
External access to systems and databases used for processing personal data takes place via secured firewall.	Inspected that external access to systems and databases used for processing personal data only takes place via secured firewall. Inspected that firewall is configured in accordance with internal policy.	No comments.
The data processor has implemented a policy – defining strength and protocol for encryption - for encrypting personal data.	Inspected the existence of formalized procedures ensuring that transmission of sensitive and confidential information via the internet is protected by strong encryption based on a recognized algorithm.	No comments.
The established technical measures are tested on an ongoing basis using vulnerability scans and penetration tests.	Inspected that formalized procedures exist for ongoing testing of technical measures, including making vulnerability scans and penetration tests.	No comments.
Supervising physical security: Physical access control is established to premises and data centres, where personal information is stored and processed.	We have asked Management whether procedures for physical security are established. We have inspected that IST Group has established an appropriate framework for operations, and that physical barriers and access control to the data centre are established. In that connection, we have inspected that supervision regarding physical security is performed at sub-processors.	No comments.
Teleworking must take place via two-factor authentication.	Controlled the existence of formalized procedures ensuring that two-factor authentication is applied when teleworking is used.	No comments.
The data processor has implemented a procedure for user administration ensuring that creating and removing of users is a controlled process and that all user creations are authorized. User rights are granted based on work-related needs. Privileged (administrative) access rights are granted to systems and units based on work-related needs. A quarterly review is performed of users and user rights. Logging is performed of all access to systems and data.	Inspected the existence of formalized procedures for limiting users' access to personal information. Inspected the existence of formalized procedures for following up whether users' access to personal information is in accordance with their work-related needs. Inspected that the agreed technical measures support the maintenance of limitation in the users' work-related access to personal information. Inspected the existence of established work tasks for ongoing review of users and user rights. Inspected the existence of formalized procedures for installation of logging user activities in systems and databases used for processing personal data.	No comments.

A uniform framework is established for the organisation's contingency plans to ensure that all plans are coherent and consider all security requirements - and to determine the prioritization of testing and maintenance.	We have asked Management whether plans for business continuity management are devised. By inspection on a sample basis, we have verified: • that appropriate framework for preparation of business continuity management has been established • that contingency plans are prepared and implemented • that the plans include business continuity management across the organisation • that the plans include appropriate strategy and procedures for communication with the customers. • that contingency plans are tested on a regular basis • that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.	No comments.

Control objective C: Organizational security measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

IST Group's control activity	Beierholm's performed test	Findings
The data processor has devised and implemented an information security policy. The data processor's information security policy is reviewed and updated as a minimum once a year.	We have in interviews asked Management about the control. Inspected that an information security policy exists, which the Management has considered and approved during the previous year. Inspected documentation disclosing that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No comments.
The data processor has established and documented a system for control of information security.	We have in interviews asked Management about the control. Inspected the existence of a formalized framework for the management for ongoing handling and control of information security.	No comments.
The data processor carries out screening of potential employees prior to employment.	We have in interviews asked Management about the control. Inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment onboarding process.	No comments.
The data processor has devised and implemented a procedure for resignation/dismissal of employees upon termination of employment.	We have in interviews asked Management about the control. Inspected procedures ensuring that resigned/dismissed employees' rights are deactivated or terminated upon termination of employment, and that assets like admission cards, pc, mobile phone etc. are returned.	No comments.
Upon resignation/dismissal the employee is informed that the signed confidentiality agreement remains valid.	We have in interviews asked Management about the control. Inspected that formalized procedures exist ensuring that resigned/dismissed employees are made aware of the continued validity of the confidentiality agreement.	No comments.
All employees are subject to confidentiality.	We have in interviews asked Management about the control. Inspected via the employment contract that the employee is subject to confidentiality.	No comments.

All employees have signed an employment contract that includes a clause about confidentiality.	We have in interviews asked Management about the control. Inspected, using a sample of 4 employees, that the employees in question have signed an agreement which includes a clause about confidentiality.	No comments.
Upon appointment, awareness training is provided to the data processor's new employees with respect to data protection and information security.	We have in interviews asked Management about the control. Inspected that the data processor provides awareness training to all employees – training including general IT security and security of processing related to personal data. Inspected, using a sample of 4 employees, that the said employees have been introduced to: • The information security policy • Procedures in relation to data processing as well as other relevant information.	No comments.
The data processor provides introduction course for new employees, including processing personal data from the data controllers.	We have in interviews asked Management about the control. Inspected that the data processor provides introduction course for new employees about processing security in relation to personal information.	No comments.
On a regular basis, the data processor provides training to the employees with respect to data protection and information security as well as handling hereof.	We have in interviews asked Management about the control. On a regular basis, the data processor provides training to the employees with respect to data protection and information security as well as handling hereof.	No comments
The data processor has appointed a data protection officer, who meets the requirements regarding appropriate competences.	Inspected documentation for the data processor's assessment whether a data protection officer must be appointed. Inspected documentation for the publication of the data protection officer's contact information. Inspected documentation for Management's processing and approval of the appointment of the data protection officer, including ensuring the data protection officer's competences.	No comments.

Management has ensured that the data protection officer is bound to professional secrecy and confidentiality in relation to performing his/her duties.	Inspected documentation proving that Management has pledged the data protection officer to professional secrecy and demands regarding confidentiality.	No comments.
The data protection officer has devised procedures in writing – updated at least once a year – in which the data protection officer's involvement, activities, and reporting is described.	Inspected the existence of updated procedures in writing regarding the data protection officer's involvement, activities, and reporting – to ensure the procedures are sufficient and updated.	No comments.
Management has ensured that the data protection officer has performed his/her duties in accordance with the available procedures, including ensuring the data protection officer's tasks at the data processor.	Inspected documentation proving that Management has ensured that the data protection officer has performed his/her duties according to the available procedures, including ensured the performance of the data protection officer's tasks at the data processor.	No comments.

Control objective D: Erasing personal data

Procedures and controls are complied with to ensure that personal information can be erased or returned if an agreement is signed with the data controller in this regard.

IST Group's control activity	Beierholm's performed test	Findings
Written procedures exist which include a requirement that personal data must be stored and erased in accordance with the agreement with the data controller.	Inspected that formalised procedures are in place for storing and erasing personal data in accordance with the agreement with the data controller.	No comments.
Upon termination of the processing of personal data for the data controller, data has, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Erased if this is not in conflict with other legislation.	Inspected that formalised procedures are in place for returning or erasing the data controller's data upon termination of the processing of personal data.	No comments.

Control objective E: Storing of personal data

Procedures and controls are complied with to ensure that the data processor will only store personal data in accordance with the agreement with the data controller.		
IST Group's control activity	Beierholm's performed test	Findings
Procedures in writing exist including a requirement that personal data must only be stored in accordance with the agreement with the data controller. On an ongoing basis – and at least once a year – it is assessed whether the procedures must be updated.	Inspected that formalised procedures exist for only storing and processing personal data in accordance with the data processor agreements. Inspected that the procedures are updated.	No comments.
Data processing, including storage, by the data processor must only take place in the localities, countries or regions approved by the data controller.	Inspected that the data processor has complete and updated records of processing activities stating localities and countries.	No comments.
The data processor keeps records of processing activities as data processor.	We have in interviews asked Management about the control. Inspected that the data processor has total and updated records of processing activities.	No comments.
The records are updated on a regular basis in relation to material changes.	Inspected that the records of processing activities are updated and maintained.	No comments.
The records are updated as a minimum once a year in connection with the annual review.	Inspected the existence of an internal task in the form of a review of the records of processing activities.	No comments.
The records are stored electronically in the data processor's system/file drive.	Inspected that the records of processing activities are stored in an electronic format.	No comments.

Control objective F: Sub-processors

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of data subjects and the processing of personal data, the data processor ensures adequate security of processing.

IST Group's control activity	Beierholm's performed test	Findings
Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-processor agreements and instructions. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	Inspected that formalised procedures are in place for using sub-processors, including requirements for sub-processor agreements and instructions. We have checked that the procedures are updated.	No comments.
The data processor only uses sub-processors who have been specifically or generally approved by the data controller to process personal data.	Inspected that the data processor has a complete and updated list of sub-processors used. Inspected, using a sample of 3 sub-processors from the data processor's list of sub-processors, that there is documentation disclosing that the sub-processors' data processing is stipulated in the data processor agreements – or other ways is approved by the data controller.	No comments.
When changing the generally approved sub-processors used, the data controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the data processor. When changing the specially approved sub-processors used, this must be approved by the data controller.	Inspected that formalised procedures are in place for informing the data controller when changing the sub-processors used.	No comments.
The data processor has subjected the sub-processor to the same data protection obligations as those stated in the data processor agreement or similar document with the data controller.	Inspected the existence of signed sub-processor agreements with sub-processors used and included in the data processor's list. Inspected using of a sample of 3 sub-processor agreements that these agreements include the same requirements and obligations as are stipulated in the data processor agreements between the data controllers and the data processor.	No comments.

The data processor has a list of approved sub-processors disclosing: • Name; • Business Registration No.; • Address; • Description of the processing.	Inspected that the data processor has a complete and updated list of sub-processors used and approved. Inspected that, as a minimum, the list includes the required details about each sub-processor.	No comments.
Based on an updated risk assessment of each sub-processor and the activity taking place at such processor, the data processor regularly follows up thereon through meetings, inspections, reviews of auditor's reports or similar activity. The data controller is informed of the follow-up performed at the sub-processor.	Inspected that formalised procedures are in place for following up on processing activities at sub-processors and compliance with the sub-processor agreements. Inspected documentation disclosing that each sub-processor and the current processing activity at such processor are subjected to risk assessment. Inspected documentation disclosing that appropriate update has been performed on technical and organisational measures, processing security at the sub-processors used, basis for transfer to third countries, etc.	No comments.

Control objective G: Transfer of personal data to third countries etc.

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller as well as by using a valid basis of transfer.

IST Group's control activity	Beierholm's performed test	Findings
Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller and by using a valid basis of transfer. On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.	Inspected that formalised procedures exist to ensure that personal data is only transferred to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. We have checked that the procedures are updated.	No comments.
The data processor is only allowed to transfer personal information to third countries or international organisations according to instructions from the data controller	Inspected that the data processor has guidelines ensuring that personal information is only transferred to third countries or international organisations in accordance with instructions from the data controller.	No comments.
The data processor has assessed and documented that a valid basis of transfer exists in connection with transfer of personal information to third countries or international organisations.	We have in interviews asked Management about the control. We have asked whether any data has been transferred to third countries or international organisations in connection with IST Group's deliveries, and we have been informed that no data has been transferred to third countries or international organisations in connection with IST Group's deliveries.	No comments.

Control objective H: Assisting the Data Controller

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, erasing, or restricting information on the processing of personal data to the data subject.

IST Group's control activity	Beierholm's performed test	Findings
The data processor has devised a procedure for assistance to the data controller in relation to ensuring the rights of data subjects.	We have in interviews asked Management about the control. Inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects.	No comments.
The Data Processor is obliged to acquire an ISAE 3000 Report regarding the technical and organizational security measures in relation to the processing and protection of personal information.	We have in interviews asked Management about the control. Inspected that IST Group acquires an ISAE 300 Report regarding the technical and organizational security measures in relation to processing and protecting of personal information.	No comments.
On request, the Data Processor provides the necessary information to the Data Controller and the Supervisory Authority in connection with audit and inspection of the Data Processor.	We have in interviews asked Management about the control. Inspected that the standard data processor agreement includes requirements to the Data Processor to assist the Data Controller and the Supervisory Authority in relation to audit and inspection.	No comments.
The data processor has established procedures in so far as this was agreed that enable timely assistance to the data controller.	We have via interview asked Management about the control. Inspected that there are procedures in place enabling timely assistance to the data controller.	No comments.

Control objective I: Data security breaches

Procedures and controls are complied with to ensure that any security breaches are responded to in accordance with the signed data processor agreement.		
IST Group's control activity	Beierholm's performed test	Findings
The data processor informs the data controller about any personal data security breaches without undue delay.	We have in interviews asked Management about the control. Inspected the existence of formalized procedures which include a requirement to inform the data controller without undue delay in the event of any personal data security breaches.	No comments.
The data processor updates the data controller about all relevant and necessary information when the information is available for the data processor.	We have in interviews asked Management about the control. Inspected that existing procedures for informing the data controllers in the event of any personal data security breaches include detailed procedures for: • Description of the nature of the personal data security breach, • Description of the probable consequences of the personal data security breach, • Description of measures taken or proposed to be taken to handle the breach on personal data security. Inspected documentation disclosing that in the event of personal data security breaches measures have been taken to handle the personal data security breach.	No comments.
Communication between data processor and data controller is documented and stored.	We have via interview asked Management about the control. Inspected that the data processor keeps records of security incidents with specifications including which incidents caused personal data security breaches. Inspected that the data processor has included any personal data security breaches occurring at sub-processors in the data processor's records of security incidents.	No comments.

The data processor has established monitoring of the system for detection of security breaches.	We have in interviews asked Management about the control. Inspected that system monitoring with alarms is established in relation to systems and databases used for processing personal data. Inspected that the data processor provides awareness training for employees in relation to identification of any personal data security breaches. Inspected documentation for monitoring network traffic. Inspected documentation for timely follow-up on logging of access to personal data.	No comments.
The data processor has devised a procedure for assessment and identification of personal data security breaches.	We have in interviews asked Management about the control. Inspected that existing procedures for informing the data controllers in the event of any personal data security breaches include detailed procedures for: • Description of the nature of the personal data security breach, • Description of the probable consequences of the personal data security breach, • Description of measures taken or proposed to be taken to handle the breach on personal data security.	No comments.
The data processor records personal data security breaches in the data breach log.	Inspected documentation from the data security breach log to ensure that data breaches are recorded.	No comments.
The data processor has established procedures for gathering experience of personal data security breaches.	Inspected that the existing procedures for handling personal data security breaches include requirements in relation to gathering experience.	No comments.
Procedures are devised to comply with the requirements of assistance to the data controller in relation to personal data security breaches.	Inspected the existence of procedures for the data processor's assistance to the data controller in relation to personal data security breaches.	No comments.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jesper Aaskov Pedersen
Director, IT audit
På vegne af: Beierholm
Serienummer: 55a3ea90-967e-4a5c-b854-37be4db4517b
IP: 212.98.xxx.xxx
2024-12-02 09:06:52 UTC

MitID

Kim Holm Larsen
Beierholm Godkendt Revisionspartnerselskab CVR: 32895468
Partner, State-Authorized Public Accountant
På vegne af: Beierholm
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2024-12-02 09:51:57 UTC

MitID

Nikoline Kofod Ravn
Chief Compliance Officer
På vegne af: IST Group AB
Serienummer: b9cfe549-94f6-4fc2-8141-83c10774214e
IP: 78.153.xxx.xxx
2024-12-02 11:37:37 UTC

MitID

Pär Ceril Mikael Folkesson
Chief Operation Officer
På vegne af: IST Group AB
Serienummer: f7c0f27b8c0535[…]111abb8918f00
IP: 217.10.xxx.xxx
2024-12-03 09:06:22 UTC

BankID