Talentech

INFORMATION SECURITY POLICY

Last updated: 9 March 2021

Talentech

Table of contents

Talentech

TALENTECH – THE FUTURE OF HR

Talentech provides scalable SaaS solutions for every step of the talent journey: Attracting candidates, recruitment, onboarding of employees, talent management, employee engagement and eventually off boarding. Our solutions support every stage of the talent pipeline, designed with personalization and flexibility in mind, with the aim of facilitating a seamless talent journey, from start to finish, in one central platform.

Talentech is committed to provide industry leading solutions with information security as our main priority. Talentech considers information and personal data as key assets, which we safeguard for ourselves and on our customers' behalf.

1 INFORMATION SECURITY POLICY PURPOSE AND CONTENT

This information security policy describes how Talentech ensures information security within our products as well as within the Talentech organisation. The policy covers Talentech's information security objectives and requirements, and the roles and responsibilities in regard to information security within Talentech. In addition, detailed information on information security within the Talentech products can be found in the technical descriptions of the products.

1.1 Information Security Management System

In order to minimise risks and to secure that information and personal data is adequately protected in Talentech products and within the Talentech organisation, Talentech has developed a set of policies, frameworks and controls to be applied to all information and personal data related services and operations. These policies and controls form the Talentech Information Security Management System, and are aligned with and based upon the controls listed in ISO 27001.

Talentech's Information Security Management System is based upon the identification of information and personal data as assets, and the objectives of protecting the confidentiality, availability, integrity and security of these assets from threats and vulnerabilities.

Objectives

Talentech has identified the following general objectives for the Information Security Management System:

- Provide secure, stable and reliable products and services to our customers

- Continuously improve and develop the information security of Talentech
- Ensure compliance with applicable laws, regulations and guidelines
- Ensure the protection of personal data
- Evaluate and mitigate the risks associated with information and personal data

The objectives are aligned with Talentech's overall business objectives, strategies and plans.

Responsibilities

The Chief Technology Officer is responsible for information security within Talentech, and for ensuring that the Information Security Management System is updated, fit for its purpose and aligned with Talentech's business objectives. The Chief Technology Officer is also responsible for information security training within the organisation, and for reporting information security related risks to management.

The Compliance Manager is responsible for the privacy and GDPR compliance within Talentech, and for identifying, assessing and mitigating risks related to personal data processing. The Compliance Manager is also responsible for privacy training within the organisation, and for reporting privacy related risks to management.

The Development Managers as well as each business unit within Talentech are responsible for the implementation of information security and privacy policies and guidelines, as well as information security and privacy training.

Each individual Talentech employee is responsible for complying with information security and privacy policies and guidelines, and for reporting any information security or privacy risks that they identify.

Risk Management Process

In order to mitigate the risks related to information and personal data, Talentech has implemented a risk management process as a part of the Information Security Management System. The process involves the assessment of risks related to the confidentiality, availability and integrity of assets, dissemination of knowledge to relevant stakeholders of such risks, and the mitigation of the risks.

The risk management process is conducted by the Information Security and Compliance Team, consisting of the Chief Technology Officer (CTO), the Compliance Manager and the Chief Financial Officer (CFO). The Information Security and Compliance Team holds quarterly meetings where risks related to the operations of Talentech are identified, assessed and mitigated. The impact and probability of the risks are assessed and compared to the relevance, cost and impact of the mitigation measures. The Information Security and Compliance Team reports findings and actions to the Talentech management team, and conducts information dissemination activities amongst employees.

Security Incident Management

In order to ensure swift, efficient and compliant handling of incidents related to information or personal data, Talentech has implemented incident response processes that constitutes an important part of Talentech's Information Security Management System. The processes covers incidents related to both information security and personal data breaches. The CTO and the Compliance Manager are responsible for the implementation and compliance to the processes.

Information security and privacy training

Talentech's employees receive regular training on information security, privacy compliance and policies and routines, in order to ensure that information security and privacy maintains an integrated part of Talentech's operations.

Information security training and information is administered based upon employee roles and responsibilities. In addition to training, the development and product teams also test the policies and routines at least once a year, in order to ensure that the knowledge is disseminated and that the routines are updated.

GDPR and privacy training is provided as a mandatory e-learning course with a quiz-based certification. Talentech employees are required to take the course once a year in order to keep their certification. Training on policies and routines is also regularly provided and based upon employee roles and responsibilities.

2 TALENTECH'S CUSTOMERS

2.1 Information security

Talentech's goal is to provide secure, stable and reliable products to our customers. We therefore ensure that we have implemented the appropriate technical and organisational security measures needed, to protect the information related to customers. The Information Security and Compliance Team evaluate the measures continuously, and assess and mitigate the risks related to information security.

Talentech enters into written agreements with all customers. The agreements regulate the technical and organisational measures and the information security standard that Talentech has implemented in order to keep customer information secured.

2.2 GDPR and privacy

Talentech is committed to GDPR and national privacy legislation compliance. In regard to the personal data processed in Talentech's products, Talentech's customers are the data controllers and Talentech is the data processor. Talentech implements the appropriate technical and organisational security measures to safeguard the personal data trusted to us by our customers, and follows the instructions of the customers regarding the processing and protection of personal data.

Talentech enters into data processing agreements with all customers. The data processing agreements regulate the processing of personal data, including the categories of data and data subjects, sub-processors and handling of personal data breaches.

2.3 Talentech's Data Protection Officer

In order to ensure GDPR and national privacy legislation compliance, Talentech has appointed a Data Protection Officer (DPO). The DPO is available to customers for information or dialogues on privacy and personal data processing, and can be contacted on legal@talentech.com.

3 TALENTECH'S OPERATIONS

3.1 Hosting environment

Talentech provides SaaS solutions for the talent journey. In order to provide industry leading, secure and scalable solutions, Talentech hosts the SaaS solutions with ISO 27001, 14001 and 9001 hosting centre suppliers. The suppliers fulfil Talentech's requirements for physical, technical and organisational protection of information and personal data.

Hosting locations

All hosting centres are located within EU/EEA, ensuring that information or personal data is not transferred outside of this area.

Hosting centre security

The hosting centres have 24/7 surveillance systems and implemented security measures to protect from, among others, intrusion, fire, temperature, humidity and water. The power supplies of the hosting centres are secured with uninterruptible power supply systems.

The hosting centres' access to data is logged and limited to selected system administrators within the suppliers' organisation.

Visitors to the facilities are logged and escorted by a responsible technician at all times. Access by visitors must be approved by the operations manager, and is only allowed to fulfil work related duties.

3.2 Development process

Software development at Talentech considers information security and privacy as part of every development phase, and follows the principles of OWASP top 10.

Development environments

Development is separated into test and production environments by means of logical and physical access controls. Customer production data is not replicated or used in non-production environments without explicit consent from the customer.

Quality assurance process

Talentech has implemented quality assurance processes defined for each product with focus on service availability, confidentiality and integrity. The processes include security and load tests for common vulnerabilities.

Logging

To ensure adequate traceability in case of incidents and other issues, Talentech logs relevant application level events in each product.

Physical and logical user access to audit logs are restricted only to authorized Talentech personnel.

Security measures

Talentech implements appropriate and applicable technical and organisational security measures in each product, based upon risk assessments and the categories of information and personal data processed in the system. Such security measures therefore vary between the products, but often include pseudonymisation, encryption, access management, anti-malware and anti-virus programs, redundant firewalls and failed login attempts logging and limitations.

3.3 Business continuity and disaster recovery

In order to ensure the security and reliability of our products, Talentech has implemented business continuity and disaster recovery plans. The plans and routines are subject to testing at planned intervals or upon significant organizational changes, in order to ensure effectiveness.

Backup

Talentech has implemented backup routines for each product, ensuring that data can be restored if needed.

3.4 Access management

Talentech has implemented access management routines based upon the principle of least privilege. All Talentech employees have signed confidentiality agreements, and receive training in information security and privacy compliance before given access to customer information and personal data.

Access is granted to unique user identities for both Talentech, customer users and end-users. The use of shared user identities or account shall be avoided. Access is monitored and logged in accordance with the logging routines of each product.

3.5 Device and office security

The devices and equipment used by Talentech employees in their line of work, as well as the office perimeters of Talentech's, contain customer information and personal data. In order to ensure the security of this information, devices and offices must be protected in accordance with access management principles.

Talentech employees are bound by confidentiality agreements and Code of Conduct to keep all information and personal data secured.

Computers, phones and similar devices must be password protected at all times.

Talentech's offices are always locked, and accessed by key cards or similar given to Talentech employees only.

4 AUDITS OF INFORMATION SECURITY COMPLIANCE

4.1 Third party audit

In order to evaluate and improve Talentech's Information Security Management System and privacy compliance, Talentech is audited yearly by an independent third party auditor. These audits are conducted in accordance with the international standard ISAE 3000, and include revision of the information security and privacy compliance of Talentech, including quality controls, policies, routines and guidelines.

The auditor's findings are summarized in a report that is available to all Talentech customers.

4.2 Customer audit

In addition to the third party audits, Talentech's customers are entitled to conduct audits once a year in accordance with the data processing agreements. These audits shall cover the data processing Talentech is performing in the role of data processor, and can include the policies, routines and guidelines related to privacy compliance.

4.3 Third party security test

In order to evaluate and ensure compliance to OWASP Top 10, Talentech performs third party security tests yearly by an independent third party auditor.

5 POLICY IMPLEMENTATION

This Information Security Policy has been duly approved by the Talentech management, and implemented throughout the Talentech organisation.

6 CONTACT

Questions regarding the policy or Talentech's information security or privacy compliance and measures, can be referred to Talentech's Chief Technology Officer or Compliance Manager.

Thomas Hellstrøm
Chief Technology Officer
thomas.hellstrom@talentech.com

Malin Gustafsson
Compliance Manager
legal@talentech.com