IT and information security policy (GDPR) for Kontrapunkt Group

Version history

Version	Description	Date	Drafted by
V. 0.1	Initial draft	26 October 2018	Kontrapunkt Group
V.0.2	1st Edition	13 November 2018	Kontrapunkt Group
V.0.3	1 Edition	17 June 2019	Kontrapunkt Group
V.0.4	1 Edition	23 August 2019	Kontrapunkt Group

Contents

IT and information security policy for Kontrapunkt Group

Introduction

Kontrapunkt Group has an important role, in that it offers branding and identity services. Kontrapunkt Group therefore collects, processes and stores a large quantity of data, which is way it is crucial for Kontrapunkt Group's reputation and credibility that this data is adequately protected.

It is therefore a matter of importance to Kontrapunkt Group that the following are assured:

- Confidentiality - confidentiality in processing, hereunder the transmission and storage of information that is only accessible by authorised internal and external users and where users' access is limited to only what is required
- Integrity - reliable, correct functionality within our IT systems, to minimise the risk of incorrect information as a consequence of internal and external situations
- Accessibility - the accessibility and capacity of our IT systems must reflect our own requirements and those of our customers for well-functioning IT systems and access to information.

Kontrapunkt Group's executive has therefore adopted this IT and data security policy (hereinafter referred to as "IT security policy"). The IT security policy comprises the combined basis as authorised by the company's executive for IT security work within the Kontrapunkt Group.

IT security is defined in the following as being all security measures having the purpose of protecting electronic data, information and It-related assets used by Kontrapunkt Group.

Purpose

The purpose of this IT security policy is to:

- establish the overall framework for IT security, taking into consideration the risk as perceived by Kontrapunkt Group
- establish a clear allocation of responsibilities and the prudent management and control of IT security
- to ensure that Kontrapunkt Group's business-critical and personally identifiable data is collected, used and stored in compliance with current legislation.

Construction

IT security work within the Kontrapunkt Group is divided into the following key areas:

- The IT security policy describes the overall framework for IT policy in the Kontrapunkt Group.
- IT business and other procedures are the specific instructions that must be followed by employees in their daily work, such as authorisation flow.
- Operational and outsourcing guidelines describe the detailed rules and checks, such as minimum security requirements for system parameter configuration. This will be applicable to internal operations and operations performed by external parties.

Risk management

To focus the endeavours of the work on IT security that we are doing within Kontrapunkt Group, we are working according to a structured approach to risk management. The result of the risk management, including evaluation of risks, has to be reported periodically to Kontrapunkt Group's management.

The board is informed immediately of any significant deviations in the current threat scenario and the resultant adjustments in relation to areas of initiatives and the various checks. Ordinary deviations are periodically collected and reported by management.

Deviations

As a rule, the IT security policy, rulebook and guidelines must always be followed. Situations can, however,

arise whereby specific circumstances require a deviation from current security rules. A deviation of this type is based on a specific assessment and requires specific dispensation. Dispensations must be approved by the executive of Kontrapunkt Group and must be justified and supported by a risk assessment. A dispensation is always limited to a specific event and period of time.

Auditing and follow-up

It is the task of the IT security manager to ensure that, at least once annually and on the basis of the perceived risk, a systematic review and assessment should be performed of whether the IT security policy needs to be updated. The IT security manager should update the IT security policy if necessary, as well as any underlying guidelines and procedures.

Publication

The IT security policy is accessible to all Kontrapunkt Group employees via the Intranet. Guidelines and procedures are available to employees and IT sub-contractors who require them in a work-related capacity.

Personal data protection

Personal Data Policy

Kontrapunkt Group processes the personal data of our customers and employees in compliance with this data policy.

The data subject's rights

Kontrapunkt Group fully respects the rights and wishes of data subjects for the confidentiality of personal data that is submitted/collected in relation to Kontrapunkt Group's work and processing. We are attentive to the need for the protection and responsibly processing of all personal data that is submitted to us/that we collect.

Personal data encompasses all information that can be used to identify a person, including but not limited to: the person's first names and surname, age, gender, private address or other physical address, email address or other contact details, salary information, health information if relevant etc.

Kontrapunkt Group processes our customers' and employees' information within the context of our work and we delete all submitted information beyond contact details such as name, telephone and email address. This information is stored for six months, or for as long as our obligations/partnership endures.

Only employees of Kontrapunkt Group or our partners, who have been specifically allocated to a specific task, are able to access personal data and only to the extent that is required to perform the tasks that we have agreed or otherwise are obligated to perform.

Documentation of personal data processing

Because Kontrapunkt Group is obligated to be able to document our processing of personal data, it is therefore important that we always follow the workflows and procedures that describe our processing of personal data. The processing of personal data must also only be performed in the IT systems that are authorised for such a purpose.

Risk analysis and security requirements

If we introduce new workflows or IT systems that have the potential to process personal data as part of the work that we do, we must perform and document a risk analysis. This risk analysis must clearly show the potential consequences to the data subject of the relevant processing.

If a risk assessment shows increased risk to the data subject, checks must be implemented that will help to reduce risk to acceptable levels.

Security breaches
Any security breaches must be reported to the supervisory authority without delay, within a maximum of 72 hours. For telecom, a 24 hour deadline applies. If a security breach can have consequences for the data subject, we must inform the latter of this within the same deadlines.

Exchange of personal data
We only disclose data to those authorities we are obligated to inform by law, such as CPR and salary information.

IT security requirements

A number of overall IT security requirements have been determined, which should contribute towards there being a basis to maintain the anticipated level of security. The level of security is assured by:

- anchoring IT security at management level
- a precise determination of how Kontrapunkt Group will live up to all legislative and authority requirements
- placing an unambiguous responsibility within the organisation for all areas affected by the IT security policy and ongoing activities to provide information
- instructing all employees in the aspects of the IT security policy, IT business and other procedures etc. that are of relevance to their work area
- determining interfaces and allocations of responsibilities with operational suppliers
- external partners are aware of and undertake to comply with current IT security policies, transaction workflows, rules and guidelines in their collaboration with Kontrapunkt Group
- ongoing compliance checks with important IT sub-contractors that Kontrapunkt Group's requirements are met, as well as an ongoing assessment of sub-contractors' competence to perform the task in question

Working with a risk management model
To safeguard Kontrapunkt Group against the negative consequences of IT threats, our work on IT security should be based on a risk assessment of the threats identified by Kontrapunkt Group, by:

- structured collecting and evaluation of potential threats. These should be analysed periodically. There should also be an ongoing consideration of how to deal with these risks and threats.
- operations suppliers having a primary role in the preparation of risk assessments in relation to the development projects and operations for which they are responsible. Suppliers are thus responsible for collecting and reacting to altered risks and new security incidents and communicating these to Kontrapunkt Group.
- Kontrapunkt Group must require of partners and suppliers that they have prepared and are able to document IT contingency plans and that such plans hare tested in partnership with Kontrapunkt Group. Tests must be approved by Kontrapunkt Group's IT security manager.
- the establishing of contingency plans that include measures to restore business systems. These measures are also applicable to breaches of confidentiality and integrity.

Protection of information and assets
Kontrapunkt Group should be represented as being a reliable organisation that ensures that its IT services are accessible and that data is protected. This is assured by:

- basing new data security-relevant acquisitions on business-dependant needs, subject to an introductory risk assessment.
- progressing development and IT system changes according to a documented process which describes Kontrapunkt Group's needs and requirements. The process must ensure operational

stability, traceability and the ability to test the system. The process must also ensure that system, operational and user documentation are prepared.

- the identification and processing in a legal, business and ethically correct manner of all personally sensitive, business-critical and confidential data. Data is evaluated in a life cycle from registration, processing and storage through to disposal.
- assurance by a system owner that systems are specified, tested and implemented and that checks are implemented in a manner corresponding to the risk situation.
- protection of the IT environment against undesired events such as physical damage, operational interruptions, losses and unauthorised changes and use.
- prevention of all unauthorised access to the IT environment and maintenance of secure segregation of duties.

Distribution of roles and responsibilities

To assure segregation of duties and anchoring of responsibility for IT security in the Kontrapunkt Group, the primary responsibilities for data security are described below:

The executive board's responsibilities

The board ensures compliance with the IT security policy. In this context the board is responsible for:

- making available the required frameworks and resources in order to achieve the desired level of security
- ensuring the implementation of a relevant IT security policy
- acting as necessary in the event of serious security breaches
- ensuring compliance with the IT security policy and the required implementation of the IT security policy through business flows, procedures and guidelines
- establishing a common understanding throughout the organisation that IT security is a shared responsibility and that guidelines, business flows etc. are applicable to all internal and external parties
- ensuring that roles and responsibilities are described and designated within the Kontrapunkt Group internally and towards partners and suppliers
- launching IT security initiatives
- authorising and prioritising all business-critical IT systems in a contingency situation
- preparation of deviation reports to the board of directors.

IT security manager

The IT security manager has the day-to-day operational responsibility for IT security, hereunder:

- the continuous work with and further development of IT security levels at Kontrapunkt Group to assure that they are in compliance with the requirements of the IT security policy. This encompasses all associated business procedures and guidelines, as well as compliance with current legislation, including executive orders and instructions applicable to the sector.
- ensuring that suppliers comply with the requirements for outsourcing agreements, including that the basis for agreements with suppliers is in compliance with the IT security policy insofar as concerns checks, follow-up and reporting
- ongoing monitoring and reporting of any IT-security-related incidents in compliance with the rules established in this IT security policy.
- launching own investigations or testing to the extent it is deemed necessary.
- assumption of a role as overall IT security co-ordinator.
- functioning as contact for external auditing for the purposes of IT audits.

Business owner, system owner and data owner

There are three central roles within the Kontrapunkt Group in relation to IT usage.

Business owner: The business owner is the business's representative as regards IT and is responsible for ensuring that business and IT are in alignment.

System owner: Is responsible for the operation and development of the system, including approving security surveillance level, logging level for security-relevant areas and backup levels in relation to the requirements of the business.

Data owner: Is responsible for ensuring that data within the system is processed in an appropriately secure manner and that risk assessments and classifications have been prepared. The data owner is also responsible for determining frameworks for access allocations that will be the task of the IT operational supplier or system administrator to perform.

Employees

Our employees are Kontrapunkt Group's most important developmental and operational resource, which also means that they represent the biggest single threat to the security of our data. Focus on compliance with the IT security policy and

preparation of employee instructions for the individual areas are therefore crucial to Kontrapunkt Group.

Each Kontrapunkt Group employee has a shared responsibility for IT security and is obligated to comply with the rules established in the IT security policy, with associated business and other procedures, as well as guidelines etc.

Infractions can be considered as a breach of the employee's terms of employment, based on a specific evaluation of each case.

Outsourcing

Kontrapunkt Group may decide to outsource activities, including the use of cloud solutions. Outsourcing of significant areas of activity is only permitted after a board decision to do so, taking into consideration all relevant legislative requirements and other regulatory provisions.

The outsourcing contract

The contract must contain an IT security instruction that describes the desired level of IT security for Kontrapunkt Group's systems and data, as well as a stipulation that the operating supplier shall comply at all times with Kontrapunkt Group's IT security policy and ruleset. Kontrapunkt Group shall ensure ongoing control and follow-up of the aforementioned compliance.

The IT deliverable

The IT supplier shall ensure that the IT deliverable is performed in accordance with recognised "good IT practice" for the relevant areas, hereunder daily administration, system planning, surveillance, management of any changes, reporting etc.

Kontrapunkt Group is responsible for following up that the IT service corresponds to the expectations and requirements set by Kontrapunkt Group.

IT auditing

When outsourcing significant areas of activity, the IT supplier shall ensure that its external IT audit shall report at least once annually to Kontrapunkt Group about the IT supplier's current level of IT security.