Data Protection Policy

TietoAkseli Group as Data Processor

Tero Anttila

21 tammikuu 2021

Version: V1.5

Status: Accepted

Classification: Public

Contents

Version history

Version	Date	Modified by	Notes
V1.0	5 April 2018	Tero Anttila	Publication of the new data protection policy.
V1.1	27th October 2018	Tero Anttila	Updated chapter 3.
V1.2	17th March 2019	Tero Anttila	Visual update
V1.3	10th June 2020	Tero Anttila	Updated chapter 3.
V1.4	21th January 2021	Tero Anttila	Visual update
V1.5	21th January 2021	Tero Anttila	Updated chapter 3

Last edited

Tero Anttila
21.1.2021 13:41

Data protection policy: TietoAkseli as processor

1 Purpose of the data protection policy

This data protection policy implements a process of transparent information, communication, and modalities in the exercise of the rights of the data subject as stipulated in the EU General Data Protection Regulation (GDPR) (EU, 2016/679) with which any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 which relates to processing and which is conducted with the data subject should be delivered to that data subject in a concise, transparent, intelligible, and easily-accessible form, using clear and plain language.

TietoAkseli Group is an expert in financial administration, providing financial administration services to its clients. When an organisation outsources the management of its financial administration services to TietoAkseli, at the same time it outsources the processing of its personal data. However, the client remains the controller of personal data as intended by the GDPR. This data protection policy describes the procedures for situations in which TietoAkseli acts as the processor of data on behalf of its clients.

2 Controller

TietoAkseli has made agreements with its clients about the production of financial administration services. For the financial administration services which are provided by TietoAkseli, the controller is TietoAkseli's client. In this data protection policy, the controller shall later on be referred to as the 'Controller'.

3 Processors

The financial administration services being provided by the TietoAkseli Group for its clients are produced by its regional, independent limited companies, but the same principles in relation to the processing and protecting of personal data applies to all companies within the group.

TietoAkseli Ltd
Business ID: 0662160-9
Registered domicile: Jyväskylä

TietoAkseli Ltd Pirkanmaa
Business ID: 1453025-6
Registered domicile: Tampere

TietoAkseli Group Ltd
Business ID: 2272844-9
Registered domicile: Jyväskylä

TietoAkseli Audit Ltd
Business ID: 2243346-4
Registered domicile: Jyväskylä

TietoAkseli Corporate Finance Ltd
Business ID: 2269964-1
Registered domicile: Jyväskylä

Within this data protection policy, the processor of personal data hereinafter is referred to as 'TietoAkseli'.

4 The contact point for the processor

The contact point in all questions that are related to data protection is:

TietoAkseli Group
Tero Anttila, Privacy Officer
+358 10 347 2831
+358 10 347 2800 (exchange)
privacy@tietoakseli.fi
Puistokatu 2 C, FI-40100 Jyväskylä, Finland

5 TietoAkseli Group as an organisation

TietoAkseli Group is an accounting service provider which specialises in the provision of financial administration services. For example, we offer our clients payroll services and human resources development services. The TietoAkseli Group also includes TietoAkseli Corporate Finance, which specialises in company reorganisation and TietoAkseli Audit, expert company specializing in auditing services.

Processing confidential personal data and other confidential information is part of our everyday work. Therefore we also take data protection and information security issues seriously. We have consistently developed the quality of our operations over the years, even before the GDPR such as, for example, in the following ways:

- TietoAkseli Group is an authorised accounting company which is supervised by the Association of Finnish Accounting Firms. Our expertise, information systems, and operating methods are of the industry's highest standard, and we have all appropriate liability insurances in place to cover our operations. The expertise of our staff is always up-to-date and current.

- TietoAkseli's quality management system is certified in accordance with the ISO 9001 standard. Customer satisfaction is extremely important to us, and we improve our operations continuously. As a TietoAkseli client, you can count on our methods of operation to be efficient and to the purpose.

- TietoAkseli is a forerunner in electronic financial administration. We have reached the highest level in Procountor International's partnership programme and are an official Lemonsoft partner. We can implement even complex integration and implementation projects for electronic financial administration.

- TietoAkseli is the only Finnish company to have been accepted for membership of UHY International, one of the world's leading networks of business management and financial administration companies. We offer our services to Finnish subsidiaries of international companies as well as to Finnish companies which operate in a global environment.

- TietoAkseli is one of the first companies in Finland to have certified its operations in accordance with the FINCSC cyber-safety certificate. FINCSC is a certification system which has been created for companies and communities to secure the continuity of their businesses. The use of the system ensures that organisations are capable of maintaining information safety and data protection and also guarantees operational and reliable services to the partners and clients of such organisations.

6 Other processors

TietoAkseli and the Controller have drawn up a written agreement which covers the processing of personal data (Data Processing Agreement, DPA). The agreement states that TietoAkseli may use subcontractors for the processing of personal data. Here, the term 'Subcontractor' refers to processors who process personal data in accordance with this agreement, wholly or partially, on behalf of the Processor and at the Processor's request.

In practice, the Subcontractors are often our ICT partners and other partners with technical access to the information systems which are managed by TietoAkseli or the facilities which are required for their maintenance. As a rule, all expert work which is carried out in the production of the Controller's financial administration services is handled by TietoAkseli's own experts.

The list of Subcontractors being used by TietoAkseli will be provided to the Controller upon request. TietoAkseli will inform the Controller of any planned changes regarding any amendments or additions to the number of Subcontractors. An appropriate confidentiality agreement has been made with all Subcontractors.

7 The purpose of processing personal data

TietoAkseli and the Controller have entered into an assignment contract in accordance to which the Controller will acquire from TietoAkseli the services described in the contract. TietoAkseli will process the Controller's personal data in order to produce its financial administration services on behalf of

the Controller. The purpose of the assignment contract is usually to implement the Controller's compliance with its statutory obligations both as an organisation and an employer. In addition, TietoAkseli may produce for the Processor expert services within which personal data is also processed.

The Processor can, for example, be a private trader, a general partnership, a limited partnership company, a limited company, or a cooperative, foundation, or association. The services which are provided by TietoAkseli, which may contain the processing of personal data, include the following:

- Financial administration services which are provided for the implementation of the organisation's accounting, financial statements, and tax return services
- Financial administration services which are provided for the organisation's payroll administration and human resources management services
- Financial administration services which are provided for the organisation's invoicing and accounts receivable services
- Financial administration services which are provided for the organisation's settlement services and accounts payable services
- Services which are related to the organisation's determination of value, Due Diligence, and company reorganisations
- Other expert services and services which are related to the auditing of accounts
- Electronic financial administration services and other data management services for the organisation

No automated individual decisions or profiling, which may have legal consequences or similar significant effects for the data subject, will be used in the processing of personal data.

8 The legal grounds for processing personal data

The processing of personal data which is carried out by TietoAkseli is always based on an assignment contract between the Controller and TietoAkseli and a contract for the processing of personal data. The processing of personal data is often required in order to comply with the statutory obligations of the Controller, for the purposes of carrying out the obligations, and in exercising the specific rights of the Controller or of the data subject in the field of employment and social security and social protection law, or in implementing the legitimate interests of the Controller.

9 Categories of personal data

Depending upon the content of the assignment contract between TietoAkseli and the Controller, TietoAkseli may process personal data in the following categories for data subjects:

- The earners of salaries and fees, in order to produce payroll and human resource management services
- The personal data of the Controller's consumer clients for the production of invoicing and accounts receivable services

- The Controller's shareholders and partners for the implementation of the organisation's administration, accounting, financial statements, and tax returns
- The Controller's shareholders and partners as well as earners of salaries and fees for the performance of Due Diligence operations or a reorganisation
- The members of the Processor (in terms of associations) for the implementation of the organisation's administration
- The residents of the Processor (in terms of housing associations) for the implementation of the organisation's administration

10 Categories of personal data

Depending upon the content of the assignment contract between TietoAkseli and the Controller, TietoAkseli may process the following personal data for the key categories of data subjects:

- Full name
- Complete address, phone number, and email address
- Position in the organisation
- Bank account details
- Services used by personal customers
- The collection and itemisation of working hours monitoring
- Employment information
- Salary information and the grounds for the determination of salary in terms of employment
- Employment payslips
- Employment salary transactions and statistics
- Employment holiday information
- Absences during employment
- Annual leave days owed due to length of service
- Employment contract
- Tax card information

11 Special categories of personal data

The special categories of personal data and other information which can be interpreted as being of a confidential nature as intended by the GDPR will mainly be processed in the salary and human resources management services. In addition, the personal identity code will be used in the identification of the actual beneficiaries in the organisation, for notifications being made to the authorities and, for instance, in shareholder registers.

Processed special categories of personal data and other data which is interpreted as being of a confidential nature may include, for instance, the following:

- Personal identity code
- Gender
- Language of communication

- Information regarding any debt recovery procedures
- Information on sick leave and absences
- Medical certificates
- Information about the employee's membership in a trade union if the employee has authorised the employer to take the membership fee directly from the employee's salary

12 Typical sources of information for personal data

The primary source of information for personal data is the Controller. The Controller saves personal data in the jointly-used financial administration information systems. Furthermore, the Controller may deliver personal data to TietoAkseli via email, phone, or verbally, or through TietoAkseli's Vina customer service system. In accordance with the assignment contract, TietoAkseli may also retrieve personal data from those information systems which are managed by the Controller. Personal data may also be received directly from the data subjects themselves such as, for instance, via email, phone, or by the data subjects themselves entering personal data into the information system.

In addition, personal data may be received from authorities, such as the Tax Administration body, the social insurance institution of Finland KELA, the Finnish Patent and Registration Office, or the enforcement authorities. Furthermore, suppliers, trade unions, unemployment benefit societies, and accident insurance companies may submit personal data.

13 Personal data recipients

The recipient of personal data refers to a private individual (a so-called natural person) or a legal entity, public authority, agency, or another body to which personal data are disclosed.

Personal data may be disclosed for the purposes of the implementation of the Controller's statutory obligations or to protect its legitimate interests such as, for instance, to the tax authorities, the social insurance institution of Finland KELA, the Finnish Patent and Registration Office, the enforcement authorities, suppliers, trade unions, unemployment benefit societies, and accident insurance companies.

By order of the Controller or with the data subject's consent, personal data can also be disclosed to other parties, such as the Controller's auditors, lawyers, and other experts.

14 Disclosure practices regarding personal data

The disclosure of personal data to third parties requires the consent of the Controller within the framework of the assignment contract, power of attorney, or through a separate request for action. TietoAkseli may also have to disclose personal data to authorities based upon statutory information requests.

A written certificate of receipt is always drafted in relation to the disclosure of manual materials. The identity and the right of the recipient to receive the materials are verified separately in connection

with the disclosure of the material. The disclosure of digital material is protected by the appropriate technical measures.

15 Technical safeguards for personal data

15.1 Technical safety

Electronically-processed personal data must be protected with appropriate data security technology. TietoAkseli data communications takes place in encrypted networks, and access to these is secured by several technical procedures, such as two-step authentication. The data systems and the data within the systems are safeguarded with firewalls, anti-virus solutions, intrusion detection and prevention systems (IDS/IPS), and AI-based solutions which are based on behaviour analysis. The personal data being processed in TietoAkseli's email and communications solutions are encrypted both data at rest as well as in transit. Emails are encrypted based on the content and sender, as necessary. The data of TietoAkseli's clients is automatically backed up, and the backups are kept at a location which is physically separate from the production systems.

15.2 Safety of the facilities

As a rule, TietoAkseli operates in facilities with appropriate safety interlocks, access control, camera monitoring, crime alarm equipment, and a guarding system. Visitors are only permitted in the facilities under escort. Employees observe the clean desk policy at their working spaces.

15.3 The processing of manual personal data

Any customer data and related personal data stored in a manual format are kept in locked facilities. The client's property is managed and protected in accordance with the ISO 9001 standard. A written certificate of receipt is always made for the disclosure of manual materials. The identity and the right of the recipient to receive the materials are verified separately in connection with the disclosure of the materials.

16 Organisational protection measures for personal data

16.1 The foundation for organisational protection measures

TietoAkseli's quality management system is certified in accordance with the ISO 9001 standard. The ISO 9001 standard observes a process-based operation model which also involves the so-called PDCA cycle (Plan, Do, Check, Act) and risk-based thinking.

TietoAkseli plans its processes and their interactions with this kind of process-approach to its operational model. With the PDCA model, the organisation can ensure sufficient resources and management for its processes and can also ensure that any chances of continuous improvement are defined and utilised. With the help of risk-based thinking, TietoAkseli is able to define the factors that may cause its processes and quality management system to deviate from the planned results. Furthermore, TietoAkseli may use preventive management measures for reducing as much as possible any detrimental effects and for utilising any opportunities that may arise.

TietoAkseli operations have been certified in accordance with the FINCSC cyber-safety certificate. FINCSC is a certification system which has been created for companies and communities to secure the continuity of their businesses. The use of the system ensures that organisations are capable of maintaining both information safety and data protection, and guarantees operational and reliable services to their partners and clients.

Independent, accredited rating institutions audit TietoAkseli's quality management systems and compliance with cyber-safety requirements on an annual basis. Furthermore, TietoAkseli utilises external cyber-safety expert organisations in the development of its cyber-safety preparedness.

16.2 Personnel safety

The foundation of TietoAkseli's personnel safety is our healthy, competent, and motivated staff. Our processes where they are related to recruitment, the introduction of new employees, changes in job descriptions, and the termination of employment contracts have been described, and their execution is monitored. The background, competence, and suitability for the work is ensured in terms of all employees before they are recruited. The credit records of all new employees are checked, and all new employees must pass a drugs test.

Every TietoAkseli employee has signed a separate confidentiality agreement and is thereby bound by an obligation to observe full confidentiality. Every new TietoAkseli employee participates in an orientation programme which contains separate sections such as, for instance, on the use of tools and information systems, data security and data protection, the safety of the facilities, quality management practices, the management of documented data, the management of the client's property, and the use of social media. The appropriate execution of the orientation programme is monitored.

TietoAkseli has a clearly-defined data security policy in place along with related data security and data protection practices. The data security-related competence of the staff is maintained through the use of training and informative one-off lessons.

16.3 Identity and access management

The data and the related personal data of TietoAkseli's clients may only be processed by those employees whose task it is to process such data. The processing of personal data for other purposes is forbidden.

TietoAkseli has centralised its identity and access management (IAM). Access to data systems and customer data is limited by user accounts and user rights. Access rights requests to access information systems and client data are submitted via the electronic system. The purpose and duration of any right of access must be stated in the access rights request. The employee's supervisor will process and approve any access rights request based on the actual need for any access. The body responsible for TietoAkseli's identity and access management defines and grants access rights based only on an access rights request which has been approved by the supervisors. Access rights are

audited at regular intervals. An electronic record is kept of the employee's access rights to the TietoAkseli information systems, plus those of TietoAkseli's clients and appropriate third parties. As an employee's duties change or their employment ends, access rights which are no longer appropriate will be audited and deleted.

16.4 Organisational safeguards for other processors of personal data

A separate confidentiality agreement has been drawn up with all of TietoAkseli's partners, suppliers, and subcontractors who are therefore bound by the agreement. In accordance with the ISO 9001 standard, all outsourced functions must be directed and monitored in a consistent way. The access of other personal data processors to TietoAkseli's clients and the related personal data is monitored and managed.

17 The location of personal data

As a rule, the personal data which is contained within TietoAkseli's information systems and personal data files are stored in Finland. The data from TietoAkseli's email service, other communications solutions, and Business Intelligence systems are stored in the EU region. The data of the software being used in TietoAkseli's client information and marketing communications is stored in the data system of a service provider which is based in the USA. As a rule, these information systems are not used to process special categories of personal data, as defined in the GDPR. The system is protected in accordance with the EU-US Privacy Shield framework.

18 The transfer of personal data

As a rule, TietoAkseli does not transfer the Controller's personal data outside the European Union, the European Economic Area, or other countries which the European Commission has found are able to guarantee a sufficient level of data protection.

Any transfer of personal data outside the European Union, the European Economic Area, or other countries which the European Commission has found to guarantee a sufficient level of data protection may only take place at the request of the Controller.

TietoAkseli and the Controller have agreed that in its customer and marketing communications, TietoAkseli may use information systems and tools for which data that is contained within them is saved on servers which are located in the United States. As a rule, such information systems and tools are not used to process special categories of personal data, as defined in the GDPR. The systems are protected in accordance with the EU-US Privacy Shield framework.

19 Storage period and the removal of personal data

The Controller's accounting material contains personal data. The legislation decrees the following regarding the storage of accounting materials and payroll accounting:

- In accordance with the Accounting Act (*Kirjanpitolaki*, 1336/1997), the financial statements, management report, ledgers, the chart of accounts, and the list of ledgers and materials must be retained for at least ten years from the end of the financial year.
- The vouchers for the financial year, correspondence regarding transactions and accounting material other than that referred to in section 10, subsection 1 of the Accounting Act must be retained for at least six years after the end of the year during which the financial year ended.
- In accordance with the Withholding Tax Act (*Ennakkoperintälaki*,1118/1996), any payroll accounting which is related to payments in accordance with the act must be retained for at least ten years from the end of the financial year. Similarly, any notes and vouchers for payroll accounting must be retained for at least six years after the end of the year during which the payment has been made.
- In accordance with the Working Hours Act (*Työaikalaki*, 605/1996), the working hours register must be retained at least until the end of the period which has been designated for claims. The designated period for claims that is referred to in the act is the previous two years in which the employment relationship is in force, and the two years after the employment contract ends.
- In accordance with the Annual Holidays Act (*Vuosilomalaki*, 162/2005), the records for annual holidays must be retained for at least two years from the end of the calendar years during which the holidays should have been granted, and two years after the employment contract ends.

If, for example, social security compensation has been granted (by Kela) based on the production of medical certificates for one of the Controller's employees, these certificates are documents that must be stored for six years.

The statutory obligation for retaining accounting material therefore limits the data subjects' right to execute all of the rights which have been granted to them by the GDPR, such as the 'right to be forgotten'.

TietoAkseli attends to the appropriate storage and destruction after the set period for any accounting documents and payroll accounting materials that are in its possession.

20 The Controller's instructions to the Processor

In accordance with Article 29 of the GDPR, the processor and any person acting under the authority of the Controller or of the Processor who has access to personal data shall not process such data except upon instructions received from the controller, unless required to do so by European Union or member state law.

The Controller has, within the framework of the agreement on processing personal data between TietoAkseli and the Controller, issued separate written instructions to TietoAkseli regarding the appropriate processing of personal data. The purpose of these instructions is to ensure that the obligation of the GDPR regarding the safeguards for processing personal data are implemented, taking into account the risk-based nature of the data.

The Controller must regularly ensure that the instructions and documents are up-to-date. If there are essential changes to the Controller's or TietoAkseli's practices or information systems, their impact on the implementation of data protection will be assessed separately.

21 Realising the rights of the data subjects

In accordance with Articles 13-22 of the GDPR, the data subjects have, for instance, the following rights:

- The right to withdraw their consent for processing personal data
- The right to lodge a complaint with a supervisory authority regarding the processing of personal data
- The right to know whether automated profiling is used in the processing of personal data
- The right to obtain confirmation about their personal data being processed
- The right to obtain access to their personal data
- The right to obtain a copy of their personal data
- The right to correct inaccurate information
- The right to have personal data erased (the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object, and automated individual decision-making

The rights of the data subject are not unambiguous. On a case-by-case basis, other legislation may prevent the full implementation of the data subject's rights. For example, the statutory obligation for retaining accounting materials serves to limit the data subjects' right to execute the 'right to be forgotten' which is granted to them by the GDPR.

The rights of the data subject are rights in relation to the Controller. When TietoAkseli acts as the processor of personal data, the execution of the rights of the data subject as intended by the GDPR is always the responsibility of the Controller, ie. a client of TietoAkseli's financial administration services. TietoAkseli has no right to disclose data from the Controller's personal data record to the data subjects themselves without the consent of the Controller, with the exception of statutory information requests by the authorities.

The data subjects must direct information requests and other requests for procedures to the Controller, who acts as the client of TietoAkseli's financial administration services. In order to be able to fully execute the rights of the data subjects, in practice the Controller needs help from TietoAkseli in order to satisfy the information request. TietoAkseli implements the Controller's requests for procedures at the Controller's request and submits the requested data to the Controller. Based on the submitted data, the Controller is responsible for exercising the rights of the data subjects.

The Controllers may direct any requests for information and procedures to the contact point indicated by TietoAkseli. TietoAkseli will identify anyone who presents a request either through the electronic Tupas-identification service or manually with more than one method of identification. The

Controller must present in any request which is directed at TietoAkseli sufficiently precise and specific information as required in order to execute the information request.

22 Reporting personal data breaches

A 'personal data breach' refers to a breach of security which may lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which is transmitted, stored, or otherwise processed.

In the case of a personal data breach, the Controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, provide notification of any personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of private individuals ('natural persons'). If any personal data breach is likely to result in a high level of risk where the rights and freedoms of private individuals are concerned, the Controller must also notify the data subject of the breach without undue delay.

TietoAkseli must provide notification of any personal data breach to the Controller without undue delay as soon as TietoAkseli or its subcontractor has gained knowledge of any such breach. Unless the parties have agreed otherwise, notification shall be provided to the representative or contact indicated by the Controller.

TietoAkselin shall submit without undue delay to the Controller any information regarding the circumstances that have led to the personal data breach as well as any other related factors that are available to TietoAkseli in accordance with the Controller's reasonable request.

As far as such information is available to TietoAkseli, the following at least must be included in the notification to the Controller:

a) a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) the name of and contact information for the data protection officer responsible for data protection at TietoAkseli;
c) a description of the likely consequences of the personal data breach;
d) a description of the measures taken or which are proposed to be taken by TietoAkseli in order to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects.

Where and insofar as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

23 Changes to the data protection practices

TietoAkseli is constantly developing its data protection and data security practices. In this regard, our data protection and data security documentation are updated from time to time. The current version

of the data protection policy is at all times available to the clients of TietoAkseli in the online services indicated by TietoAkseli.

TietoAkseli Group | +358 10 347 2800 | info@tietoakseli.fi | www.tietoakseli.fi