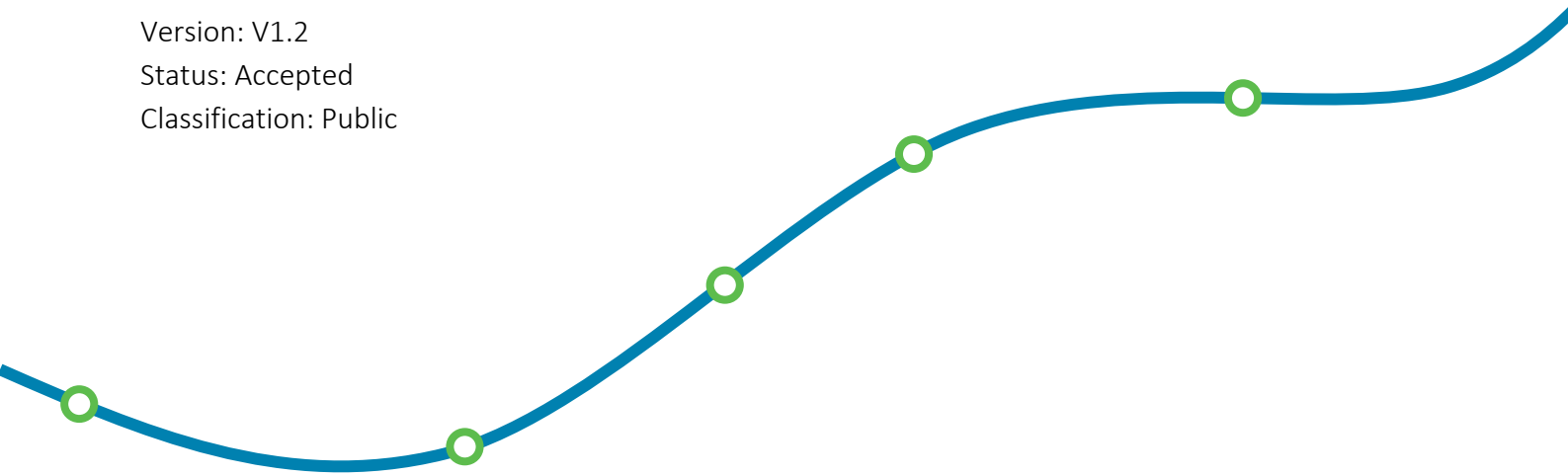
UHY TietoAkseli

Data Protection Policy

UHY TietoAkseli as a Data Controller

Tero Anttila
18 March 2019
Version: V1.2
Status: Accepted
Classification: Public



Contents

Version history

Version	Date	Modified by	Notes
V1.0	5th April 2018	Tero Anttila	Publication of the new data protection policy.
V1.1	1st October 2018	Tero Anttila	Paragraph 2 updated
V1.2	17th March 2019	Tero Anttila	Visual update

Last modified by

Tero Anttila
18.3.2019 11:48

UHY TietoAkseli data protection policy as controller

1 The purpose of the data protection policy

This data protection policy implements the transparent information, communications, and modalities for 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 communications under Articles 15 to 22 and 34 which relate to the processing of the data subject should be delivered to the data subject in a concise, transparent, intelligible, and easily-accessible form, using clear, plain language.

UHY TietoAkseli is an expert in financial administration, providing financial administration services to its clients. This data protection policy describes the principles of processing and protecting personal data with which TietoAkseli as a controller protects personal data in different situations.

When a client outsources the management of its financial administration services to TietoAkseli, at the same time it outsources the processing of its personal data. In such cases, the client is the controller of personal data as intended by the GDPR. TietoAkseli's operations as the processor of personal data on behalf of its clients is described in a separate data protection policy, 'TietoAkseli's data-protection policy as processor'. This data protection policy is available to all TietoAkseli's clients through TietoAkseli customer service system "Vina" and, as necessary, upon request.

2 Controller

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

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

TietoAkseli Ltd Etelä-Savo
Business ID: 0907155-0
Registered domicile: Pieksämäki

TietoAkseli Ltd Helsinki
Business ID: 0643871-6
Registered domicile: Helsinki

TietoAkseli Ltd Pirkanmaa
Business ID: 1453025-6

Registered domicile: Tampere

TietoAkseli Group Ltd
Business ID: 0854417-6
Registered domicile: Jyväskylä

ValueMiners Ltd
Y-tunnus: 2243346-4
Registered domicile: Jyväskylä

Vinanssi Corporate Finance
2269964-1
Registered domicile: Jyväskylä

Within this data protection policy, the controller shall later on be referred to as 'TietoAkseli' or the 'controller'.

3 The contact point for the controller

The controller's contact point in terms of any questions which are related to data protection is:

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

4 Information about our public online services

TietoAkseli has the following public services available online:

- TietoAkseli's website can be found at the address: www.tietoakseli.fi
- TietoAkseli's LinkedIn community page is at the address: https://www.linkedin.com/company/tietoakseli
- TietoAkseli's Facebook page is at the address: https://www.facebook.com/TietoAkseli
- TietoAkseli's Google+ community pages (consisting of several office-specific addresses)
- TietoAkseli's Twitter account is at the address: https://twitter.com/TietoAkseli
- TietoAkseli's Instagram account is at the address: https://www.instagram.com/uhy_tietoakseli/

These services use technology by which the user of the services can be identified, and based on this information, tailor-made services can be offered to the user.

4.1 Data encryption in transit

As a rule, our public online services use SSL-encryption in order to protect data communications between the user's device and the online service. SSL-encryption also helps to authenticate the website. Usually, you can recognise those online services that use SSL encryption by the small lock icon next to the address field in the browser, as well as by any URL that begins with 'HTTPS'.

4.2 Information about cookies

We use cookies on our sites. A cookie is a small text file which is sent to the user's computer to be stored there in order to enable functions such as the site's basic operations, for instance, and to help identify visitors to the site. Cookies are harmless and do not harm the users' device or files. With the data provided by cookies, we can target the visitor with content that is most likely to be of interest to them specifically.

If you do not want us to obtain the aforementioned information by means of cookies, please note that most browsers allow you to switch off the cookie function and to delete existing cookies. However, we ask you to bear in mind that cookies may be necessary for the smooth and most appropriate operation of the sites we maintain and the services we offer.

Learn more about the principles of browser-use-based advertising, cookies, and privacy protection, with the Your Online Choices website being one example of a source of such help.

4.3 Community plug-ins

Our websites may contain links and plug-ins for third-party websites, such as LinkedIn, Facebook, Google+, Twitter, Instagram, and other community services. The content of the sites is loaded from third-party servers. With community plug-ins, the community service providers can collect data about visits in accordance with the terms and conditions that are valid upon each visit. Read more about third party privacy policies via the following links:

LinkedIn Privacy Policy
Facebook Privacy Policy
Google+ Privacy Policy
Twitter Privacy Policy
Instagram Privacy Policy
AddThis Privacy Policy

5 UHY TietoAkseli as an organisation

UHY TietoAkseli 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 Odeco Oy, which specialises in personnel development services, and Vinanssi Corporate Finance, which specialises in company reorganisation.

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:

- UHY TietoAkseli 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 Processors

As a controller, TietoAkseli may use subcontractors in its operations. Here, the term 'subcontractor' refers to a processor who processes 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, almost without exception, 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 for the production of TietoAkseli's financial administration services is carried out by TietoAkseli's own experts.

Upon request, TietoAkseli may also provide a list which specifies the subcontractors it uses. As a controller, TietoAkseli will inform its clients of any planned changes regarding any amendments or additions to the number of subcontractors. Appropriate confidentiality agreements have been drawn up with all subcontractors.

In accordance with Article 29 of the General Data Protection Regulation (GDPR), the processor and any person acting under the authority of the controller or of the processor who has access to personal data must not process data except upon instruction by the controller, unless required to do so by European Union or member state law.

Within the framework of the agreement between TietoAkseli and its subcontractors regarding the processing of personal data (Data Processing Agreement, DPA), TietoAkseli has provided the subcontractors with separate written instructions on the appropriate processing of personal data. The purpose of the instructions is to ensure that the obligation imposed by the GDPR regarding safeguards relating to the processing of personal data are in fact implemented, taking into account the risk-based nature of the data.

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

7 The principles of processing personal data for each filing system

8 Client register

8.1 The purpose of and legal basis for processing personal data

The purpose of TietoAkseli's client register is to manage and develop TietoAkseli's client relationships. The processing of personal data which is carried out by TietoAkseli is always based on an assignment contract and a contract for processing personal data which is drawn up between the client and TietoAkseli.

The personal data in the client register is used for the production of TietoAkseli's services within the boundaries of a contractual relationship with the client, for the implementation of the client's statutory obligations, and the development of the quality of TietoAkseli's products and services. In addition, the personal data in the client register will be used for TietoAkseli's communications with its clients. The processing of personal data may also be necessary in order the exercise the legitimate rights of the controller.

8.2 Categories of personal data

Depending upon the content of the assignment contract between TietoAkseli and the client, TietoAkseli may process the personal data of the following Categories of personal data:

- Client employees, representatives, actual beneficiaries, shareholders and partners, as well as the members of the board of directors
- Client auditors and representatives in other organisations

8.3 The content of the filing system

TietoAkseli may process the following personal data for the Categories of personal data:

- Full name
- Position in the organisation
- Full address
- Telephone number, email address, instant messaging addresses
- Connections to other organisations
- Information about any communications or marketing communications bans
- Memoranda which are related to the data subject
- Calendar events which are related to the data subject
- Emails which are related to the data subject
-

TietoAkseli may also process special categories of personal data for the Categories of personal data:

- Personal identity code

The processing of special categories of personal data may be required for the purposes of identifying the actual client beneficiary, ensuring compliance with a statutory obligation, or for implementing the client's obligations and special rights.

8.4 Typical sources of information for personal data

The primary source of personal data is TietoAkseli's client and the client's representatives. Personal data can also be collected in the register from public sources of information. TietoAkseli may also complement data regarding the data subjects based on its own operations.

In addition, personal data may be received from the authorities, such as the tax authorities or the Finnish Patent and Registration Office. Furthermore, suppliers, trade unions, unemployment benefit societies, and accident insurance companies may submit personal data.

8.5 Disclosure practices and recipients of personal data

As a rule, the personal data in TietoAkseli's client contacts register is processed only within the TietoAkseli Group. Personal data is not sold, rented, or disclosed to third parties.

8.6 Storage period and the removal of personal data

The personal data in TietoAkseli's client contacts register can be stored for as long as necessary for the purpose of processing such data in order to implement the assignment contract between TietoAkseli and the client or to realise another legitimate interest. On a regular basis, TietoAkseli evaluates the legal basis of the personal data in the client contacts register. However, this will be carried out at least once a year. As and when necessary, TietoAkseli will implement procedures to remove inaccurate, expired, or unnecessary personal data.

9 Marketing register

9.1 The purpose of and legal basis for processing personal data

The purpose of TietoAkseli's marketing register is to manage and develop TietoAkseli's client relationships. In addition, the marketing register is used both for marketing communications as well as targeting official notifications to client representatives and potential clients. The marketing register is used also for processing contact and service requests which are received via TietoAkseli's online services.

For clients, the processing of personal data which is carried out by TietoAkseli is always based upon an assignment contract and a contract for processing personal data which is agreed between the client and TietoAkseli. For the representatives of potential clients and other persons, the processing of personal data is based upon the data subject's unambiguous and express consent or TietoAkseli's legitimate interest.

9.2 Categories of personal data

TietoAkseli may process the personal data of the following key Categories of personal data:

- The contact for TietoAkseli's active clients
- The contact for TietoAkseli's potential clients
- The participants of TietoAkseli's events, such as webinars and other types of event
- Persons who have downloaded TietoAkseli's downloadable content, such as guides
- Persons within TietoAkseli's cooperation network

9.3 The content of the filing system

TietoAkseli may process the following personal data for the Categories of personal data:

- The name of the data subject
- The position of the data subject within the organisation
- The data subject's address
- The phone number and email address of the data subject
- The avatar, instant messaging addresses, and social media accounts of the data subject
- Information about any communications or marketing communications bans
- Information about communications sent to the data subject

- Information about content which has been downloaded by the data subject from the TietoAkseli online services (guides, webinars, and other content)
- Information about the data subject's interests (in TietoAkseli's products, services, and events)

As a rule, special categories of personal data are not processed in marketing communications. TietoAkseli cannot with certainty prevent persons under the age of thirteen years from using TietoAkseli's public online services and sources of information. If TietoAkseli has good cause to believe that the collected data may be that of someone under the age of thirteen, the processing of the data is stopped and the data erased.

9.4 Typical sources of information for personal data

The personal data of the representatives of TietoAkseli's active clients will also be processed in TietoAkseli's marketing register unless the data subject forbids this. For the other data subjects, the primary source of information for the register is the data subjects themselves and their actions in TietoAkseli's online services. Data for the register may also be collected from public sources of information, and TietoAkseli may complement the data regarding the data subjects based on its own activities.

9.5 Disclosure practices and recipients of personal data

As a rule, the personal data in TietoAkseli's marketing register is processed only within the TietoAkseli Group. Personal data is not sold, rented, or disclosed to third parties.

In events and campaigns which are organised jointly by TietoAkseli and third parties (such as webinars and client events), personal data may be collected in the marketing contacts register, which will then be disclosed to a third party for the purposes of the practical arrangements of the event or campaign. In such cases, the data subjects are informed of the possible disclosure of the information to third parties when such information is collected.

As a rule, any processing of data which is collected in events and campaigns that are jointly organised by TietoAkseli and a third party is done electronically. The digital disclosure of personal data is protected with the appropriate technical measures.

9.6 Storage period and the removal of personal data

The personal data in TietoAkseli's marketing register will be stored for as long as is necessary for the purposes of processing the data in order to implement the assignment contract between TietoAkseli and the client, or to realise another legitimate interest. TietoAkseli evaluates the legal basis of the personal data in the marketing register on a regular basis. However, this will be carried out at least once a year. As and when necessary, TietoAkseli will implement procedures to remove inaccurate, expired, or unnecessary personal data.

10 Recruiting register

10.1 The purpose of and legal basis for processing personal data

The purpose of TietoAkseli's recruiting register is the practical implementation of the recruitment of employees and trainees at TietoAkseli. Therefore the processing of personal data is based on the express consent of the data subjects.

10.2 Categories of personal data

TietoAkseli may process the personal data of the following key Categories of personal data:

- Persons who submit their job application in connection with open vacancies at TietoAkseli
- Persons who submit an application for a traineeship at TietoAkseli
- Persons who submit an open application to TietoAkseli

10.3 The content of the filing system

TietoAkseli's recruiting register contains all of the personal data that has been submitted by the data subjects themselves. Submitted details include the subject's name, address, telephone number, email address, date of birth, gender, education, and work experience, plus their own assessment of their language skills, their desires in relation to the content of any employment contract or traineeship, the contact information of any references, as well as the information provided in any attachments, such as CVs.

10.4 Typical sources of information for personal data

The primary source of information for TietoAkseli's recruiting register is the applicants themselves. Information submitted by the data subjects may be complemented after receipt of the applicants' permission with additional details such as, for instance, information provided by applicant references or previous employers. In addition, TietoAkseli's human resources management and recruiting supervisor may complement the information during the recruitment process.

10.5 Disclosure practices and recipients of personal data

With the data subject's consent, the information can be disclosed to third parties so that a personnel assessment can be carried out. Other than for those purposes, the information in the recruiting register is not to be sold, rented, or disclosed to third parties. As a rule, the processing and disclosure of personal data for the purpose of carrying out a personnel assessment is to be carried out electronically. The digital disclosure of personal data is protected with the appropriate technical measures.

10.6 Storage period and the removal of personal data

The personal data contained in the recruiting register is to be stored for a period of 24 months from the submitting of the job application or from the last modification to the application.

11 Camera monitoring register

11.1 The purpose of and legal basis for processing personal data

All TietoAkseli offices are equipped with electronic surveillance cameras. The purpose of camera surveillance is to prevent misuse and criminal offences. Camera surveillance is used to protect the following:

- employees working in the offices
- customers and other people visiting the offices
- the personal data of clients being processed in the offices and
- the client's property where this is being processed in the offices.

Furthermore, the data saved during camera surveillance can be used to investigate cases of misuse or criminal offences in accordance with, for instance, the following legislation:

- The Protection of Privacy in Working Life Act (Laki yksityisyyden suojasta työelämässä, 759/2004)
- The Equality between Men and Women Act (Laki naisten ja miesten välisestä tasa-arvosta, 609/1986)
- The Occupational Health and Safety Act (Työturvallisuuslaki, 738/2002)

11.2 Categories of personal data

Camera surveillance records all visitors to the TietoAkseli offices.

11.3 The content of the filing system

- Video material of the area covered by camera surveillance
- The time stamp information where this is related to the video material

As a rule, special categories of personal data are not processed in a personal data file where this relates to camera surveillance. However, the video footage from camera surveillance may contain references to the special categories of personal data for data subjects.

11.4 Typical sources of information for personal data

Video footage that is recorded by the camera surveillance system and the time stamp data produced by the recording device.

11.5 Disclosure practices and recipients of personal data

As a rule, the personal data in TietoAkseli's camera surveillance register is processed only within the TietoAkseli Group and only when necessary. Personal data is not sold, rented, or disclosed to third parties.

TietoAkseli may disclose personal data taken from camera surveillance to the authorities in order to help investigate cases of potential suspected misuse and criminal offences. TietoAkseli may also be obliged to disclose the data from camera surveillance by order of a competent authority.

Upon such disclosure of personal data, a disclosure certificate must always be drafted. Any disclosure of personal data from camera surveillance is carried out electronically, and the personal data is protected with the appropriate technical measures. The data subjects shall also be informed of any such disclosure to the authorities, unless the competent authority expressly forbid it.

11.6 Storage period and the removal of personal data

The removal of video material and personal data from the personal data file in the camera surveillance register is carried out automatically. Data that is contained in a camera surveillance personal data file is stored for one year at most, unless there is an acceptable reason for storing an individual piece of personal data for a different period of time.

12 Technical safeguards for the personal data

12.1 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.

12.2 The safety of facilities

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

12.3 Processing manual personal data

Customer data and related personal data where this is 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 disclosure 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 material.

13 Organisational protection measures of personal data

13.1 The foundations 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 operations model, one 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 on its operational model. With the PDCA model, the organisation can ensure sufficient resources and management for its processes while also ensuring that any chances for continuous improvement are defined and utilised. With the help of risk-based thinking, TietoAkseli is able to define those factors which 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 in utilising any opportunities that may arise.

The 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 information safety and data protection and also guarantees operational and reliable services to the partners and clients of such organisations.

Independent, accredited rating institutions audit TietoAkseli's quality management systems and its 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.

13.2 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, 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 in place a clearly defined data security policy and related data security and data protection practices. The data security-related competence of the staff is maintained through training and informative one-off lessons.

13.3 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.

13.4 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 processors of personal data to TietoAkseli's clients and related personal data is monitored and managed.

14 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.

15 Transferring personal data

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

TietoAkseli has agreed with its clients that, in its client information and marketing communications, TietoAkseli may use information systems and tools, with any data which is contained within these systems or tools being saved on servers which are located in the United States. The same information systems are also used for targeting marketing communications at potential clients. 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.

16 Realising the rights of the data subjects

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

- 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 any processing
- The right to data portability
- The right to object to the processing of personal data 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. TietoAkseli has the right and the obligation to refuse to implement the rights of the data subjects as such, should the applicable legislation limit those rights. In such situations, TietoAkseli shall inform the data subject clearly of any grounds for a refusal and provide the data subject with guidance on how best they can fully implement their rights.

The data subjects can direct their requests for information and procedures to the contact point indicated by TietoAkseli. TietoAkseli will identify anyone who presents a request for a procedure or for information either through the electronic Tupas-identification service or manually with more than one method of identification. In any request which is directed at TietoAkseli, the data subject must present sufficiently precise and specific information, as required in order to execute the information or procedure request.

The information which is submitted in accordance with Articles 13 and 14 and all information and procedures which are based on Articles 15-22 and 34 of the GDPR are free of charge for the data

subject. If requests issued by the data subject are clearly unreasonable or unfounded, particularly if such requests are being made constantly, TietoAkseli may either

1) charge a reasonable fee, taking into account administrative costs that may be incurred by the delivery of the requested information or messages, or the administrative costs involved in completing the requested procedure; or
2) refuse to carry out the requested procedure.

In such cases, TietoAkseli must show the data subject why the request is clearly unfounded or unreasonable.

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, unless requested to do so by a statutory information request which is issued by a competent authority.

When TietoAkseli acts as the processor of personal data, the data subjects must direct any 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 exercise the rights of the data subjects, the controller in practice 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.

17 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 cases in which a personal data breach occurs and results in a high level of risk to the rights and freedoms of private individuals ('natural persons'), TietoAkseli shall proceed as follows:

- In accordance with the provisions of Article 33 of the GDPR, TietoAkseli shall inform the competent supervisory authority of the breach without undue delay and, if possible, within 72 hours of having learned of the breach;
- Furthermore, TietoAkseli must also inform the data subject of the personal data breach without undue delay, in accordance with the provisions of Article 34 of the GDPR;
- In addition, TietoAkseli shall undertake any necessary actions to prevent any risks which may be related to and which may mitigate any detrimental effects caused by the personal data breach.

18 Changes to data protection practices

TietoAkseli is constantly developing its data protection and data security practices. In this regard, our data protection and data security documentation is updated from time to time. The current version of the data protection policy is at all times available via the online services indicated by TietoAkseli.