# Talenom Plc. Description of Data Protection and Descriptions of Registers

TALENOM

yrittämisen iloa

# TALENOM DESCRIPTION OF DATA PROTECTION

| | |
|---|---|
| **Last updated** | 30th August 2018 |
| **Scope** | This Description of Data Protection describes the data security and data protection practices, processes and technology that Talenom uses to protect its customers' data. The description applies to Talenom's website, digital services targeted at customers and the production systems for financial management services. |
| **Limitations** | This Description of Data Protection does not apply to third-party websites, applications or services that may be available through the additional services of partners offered as part of Talenom's services. By opening a partner website, the customer exits Talenom's service, in which case a third party can collect and share information about the customer. Talenom recommends that before agreeing to the collection and use of his or her personal data in any third-party service, the customer should always review the data protection practices of the service in question. |
| **Data protection principles** | Talenom's data protection principles include communicating the purpose of data processing and the criteria for making data processing legitimate, protecting the data by technical, administrative and physical means, as well as providing the statutory right of access and right to request changes to the data. |
| **Personal data Registers and descriptions of Registers** | Description of Register – Marketing Register<br>Description of Register – Customer Data Register<br>Description of Register – Personal Data Register for Specialist Services<br>Description of Register – Video Surveillance Data Register in Oulu<br>Description of Register – Phone Call Recordings<br>Description of Register – Recruitment Register<br>Description of Register – List of Shareholders |
| **Processing of personal data on behalf of the controller** | In some of its services, Talenom will process personal data on behalf of a customer. In such cases, the customer is the controller of the personal data Register thus created and Talenom is the processor of personal data as referred to in the EU General Data Protection Regulation (GDPR). The measures related to the processing of personal data are always agreed on a case-by-case basis with the customer, using the *description of the measures for processing personal data* included in this document:<br><br>Description of the measures for processing personal data |
| **Technical protection of data Registers** | Data contained in personal data Registers that are processed electronically are protected by technical means: using firewalls and passwords, offering Talenom's customers two-step verification to the customer information systems and using other technical means generally accepted in the security industry. Data transfer between the customer and Talenom is encrypted using Transport Secure Layer (TLS) technology in the following Talenom services: Talenom Online, Talenom App, Mezo and Talenom Link. Data are backed up regularly and backups are stored in a separate location from the primary data.<br><br>Talenom conducts internal and third-party assessments that cover both the technical security of critical information systems and the processes and guidelines related to administrative data security and data protection. |
| **Administrative protection of data registers** | Only identified Talenom employees and the employees of companies operating on behalf of Talenom have access to the data contained in the registers, based on access rights granted to them. The access rights of users are monitored regularly, and the user access management policy prohibits the creation of dangerous combinations of access rights. The access rights of the administrators of various systems, in particular, are reviewed regularly and removed when the user no longer needs them. The access rights of departing employees will be deleted from all systems at the termination of employment.<br><br>Customer data are only processed by the employee assigned to that particular task. |

| | |
|---|---|
| | Processing customer data on any other grounds is prohibited, even if the employee has technical access to the data due to his or her role or for business reasons.<br><br>All Talenom employees, and any external persons operating on behalf of Talenom, are bound to secrecy regarding all customer and personal data held by Talenom. The obligation of secrecy, including sanctions, is specified in the employment contracts of Talenom employees and agreements concluded with third parties.<br><br>Employees who process the data of Talenom's customers receive regular training, a key part of which is the criteria for making data processing legitimate. Data security and the data protection awareness of Talenom employees is maintained regularly by various means: By holding regular information sessions on the subject for all personnel and by organising an annual mandatory training course at the end of which employees must pass a test in order to complete the training.<br><br>Talenom has an information security policy that every new employee must read through when joining Talenom. Employees are informed of the existence and location of the information security policy, and reminded of its binding nature, at regular information security training sessions. The information security policy describes the general rules for information security and data protection that are binding on employees, including technical rules, information security processes, as well as practices and guidelines applicable to daily work. |
| **Physical protection of data registers** | Customer data are processed in information systems located in a data centre in Finland or in Cloud Services within the European Union, excluding email messaging system used for delivering customer promotional communication material and statistical analysis of financial management systems use. In the data centres located in Finland, the most important production systems have been duplicated and placed in two physically separate data centres so as to keep the data safe and secure the continuity of service under normal and emergency conditions. The data centres have certified security practices, access control and supervision in place maintained by the service provider. Email messaging system used for customer promotional communication and statistical analysis of financial management systems use are located on servers residing in United States of America and are protected by service providers according to General Data Protection Regulation requirements. Statistical analysis data does not contain personal data identifiers.<br><br>Materials that are maintained manually are located on premises that have access control to prevent unauthorised access. The most important premises also have video surveillance, enabling the investigation and verification of possible breaches of physical security. |
| **Use of cookies** | Talenom can collect information on visitors to the Talenom.fi website and use cookies on the website. Cookies are small text files that are stored on the device used by the website visitor. Talenom uses cookies to improve the user experience of its website, assess the content used by visitors and support marketing activities. The information collected by cookies is anonymous, and cookies cannot be used to obtain data on a particular identifiable person.<br><br>Here are some examples of data that can be collected by cookies:<br>• Visitor's IP address<br>• Time of visit<br>• Pages visited and duration of visit<br>• Browser type or operating system used<br>• Referring page and subsequent page after leaving website |

| | |
|---|---|
| | The information collected by cookies can be used, for example, for targeted advertising in the Google Display Network.<br><br>By using Talenom's website, the visitor accepts the use of cookies and allows them to be stored on his or her computer. Most browsers accept cookies by default. The visitor can prevent the use of cookies by changing the browser settings, so that the browser will not allow the storage of cookies, in which case, the visitor accepts that preventing the use of cookies may affect the functionality of certain services. |
| **Rights of data subjects** | In accordance with Articles 15 to 22 of the EU General Data Protection Regulation, data subjects have the following rights:<br>1. right of access to personal data<br>2. right to rectify the data<br>3. right to erase the data<br>4. right to restrict processing<br>5. right to data portability<br>These rights apply to personal data stored in Talenom's information systems. Certain rights of data subjects are restricted by other legislation, based on which Talenom has the right and obligation to legitimately refuse to rectify or erase data, restrict processing or transmit data from one system to another. One example of such legislation is the Accounting Act, which governs the storage of payroll documents, irrespective of the rights of data subjects specified in the General Data Protection Regulation.<br><br>If a data subject wishes to access or change his or her personal data contained in a data register owned by a customer of Talenom, the data subject must submit a request to the controller to access or change the data. The controller will then handle the request with the processor, i.e. Talenom. In such cases, the controller must submit a written request to the email address provided below.<br><br>The request to access or change data must specify the personal data that the data subject wants to access and provide the name of the data register concerned. The request must be submitted by email to: rekisteriseloste@talenom.fi. Data subjects can use their statutory right of access, provided by the General Data Protection Regulation, free of charge once a year. |
| **Communicating personal data breaches** | The controller will inform the data subject of a personal data breach if the breach is likely to result in a high risk to the rights and freedoms of the data subject. The notification will describe the nature of the personal data breach and the measures taken, as provided by law.<br><br>In cases where the personal data breach concerns personal data contained in a personal data register owned by a customer of Talenom, the customer is responsible for informing the data subjects. The controller must be informed of the breach without undue delay. The notification must describe the nature of the personal data breach and the measures taken, as provided by law.<br><br>The data protection authorities must be informed of a personal data breach within 72 hours of its discovery if the breach is likely to result in a high risk to the rights and freedoms of the natural person. The notification will describe the nature of the personal data breach and the measures taken, as provided by law. |
| **Changing the Description of Data Protection** | Talenom is continuously developing its business and reserves the right to change this Description of Data Protection by providing prior notice of such changes through its digital services and other customer communications. Changes may be based on legislative amendments and compliance with the resulting requirements. |

| | |
|---|---|
| **Latest changes** | 1st November 2017: First version of Talenom's Description of Data Protection. The Description of Data Protection is based on an extract from Talenom's Customer Data Register and the documentation of data protection and data security principles and technical means of protection.<br><br>20th February 2018: Description of Data Protection updated and divided into a general part, describing the general and common protection principles of all personal data registers covered by the Description of Data Protection, and the descriptions of the various data registers. Created a new version of the Customer Data Register and moved the measures related to processing personal data that Talenom carries out as a processor acting on behalf of the controller to a separate appendix entitled *Description of the measures for processing personal data*. Added other identified data registers and descriptions of the registers.<br><br>14th March 2018: Addition of more details to the purpose of personal data processing, for Customer's accounting and receivables follow-up, for Limited company administration, for Association administration and for Housing cooperation administration.<br><br>31st July 2018: Updates to contact information, legal references, added information about customer promotional communication and statistical analysis of financial management systems use and added a register for list of shareholders.<br><br>30th August 2018: Added new personal data use case to Customer Data Register for enabling the use of data for conducting service improvement and marketing surveys. |

# DESCRIPTION OF REGISTER – MARKETING REGISTER

| | |
|---|---|
| **Name of data register** | Marketing Register |
| **Applicable legislation** | General Data Protection Regulation (EU 679/2016) and National Data Protection legislation |
| **Last updated** | 31 July 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Otto-Pekka Huhtala<br>Tel: +358 (0)20 752 5276<br>Email: otto-pekka.huhtala@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | Personal data are processed for the purpose of managing customer relationships and ensuring that the rights and obligations of the customer and the controller are met. Personal data are stored and processed in order to use customer data to target the marketing and sales of Talenom's financial management services through the controller's media and services, without disclosing personal data to third parties.<br><br>Personal data can be processed for the following purposes:<br>• Contacting a potential customer<br>• Arranging meetings with a potential customer<br>• Sending newsletters and sales materials<br>• Creating marketing communications, market surveys and opinion polls |
| **Content of data register** | The following information can be stored on data subjects:<br>• Name<br>• Phone number<br>• Email address<br>• Organisation and position<br>• Organisation's contact details<br>• Interaction history |
| **Regular sources of data** | Data are primarily obtained from the following sources:<br>• Asiakastieto.fi service<br>• Services providing public contact details<br>• Contact forms on the Talenom.fi website<br>• Varaaheti.fi service |
| **Regular disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Talenom does not sell, rent or otherwise disclose personal data to other parties.<br><br>Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data will not be transferred outside the European Union or the European Economic Area. |
| **Practices related to the disclosure of data** | If data are disclosed to the authorities, a certificate of disclosure will be drawn up and stored in customer-specific folders. The data subject will always be informed of disclosure in advance, unless otherwise ordered by the authorities. |
| **Storage and erasure of data** | Talenom will erase personal data contained in the Marketing Register at the customer's request. |

# DESCRIPTION OF REGISTER – CUSTOMER DATA REGISTER

| | |
|---|---|
| **Name of data register** | Customer Data Register |
| **Applicable legislation** | General Data Protection Regulation (EU 679/2016) and National Data Protection legislation |
| **Last updated** | 30th August 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Otto-Pekka Huhtala<br>Tel: +358 (0)20 752 5276<br>Email: otto-pekka.huhtala@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | Personal data are stored and processed for the purpose of providing Talenom's financial management services in accordance with agreements between Talenom and Talenom's customers. Personal data are processed in order to meet the obligations provided by law and those related to official processing, as well as to improve the quality of Talenom's products and services. |
| **Content of data register** | The following information can be stored on data subjects:<br>• Name, personal identity code and the required organisation data<br>• Contact details (address, phone number, email address)<br>• Customer relationship management data created in customer service<br>• Customer's services and invoicing data<br><br>Examples of user information recorded for a data subject:<br>• Device version<br>• Operating system version of device<br>• Browser version<br>• Java version |
| **Regular sources of data** | Registered customers add their own and their employees' personal data to Talenom's digital services. Personal data can be loaded from digital materials provided by the customer. Personal data will be collected in compliance with the terms and conditions of Talenom's financial management systems. Customers may disclose information regarding the service improvement and/or marketing questionnaires as part of surveys.<br><br>In addition, personal data will be collected from the tax authorities, the Social Insurance Institution of Finland, trade union organisations, lending services, enforcement authorities and other parties who provide information that must be processed in payroll accounting.<br><br>Information about the devices of the users of Talenom's digital products and online services will be collected automatically, using browser cookies or similar technologies, for the purpose of developing digital products and improving customer service. |
| **Disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Data contained in the register can be disclosed to the tax authorities, pension insurance companies, insurance companies, trade union organisations and the Social Insurance Institution of Finland or employment pension funds. Talenom can disclose personal data for subcontractors to enable service improvement and marketing surveys.<br><br>Talenom does not sell, rent or otherwise disclose personal data to other parties. |

| | |
|---|---|
| | Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data will not be transferred outside the European Union or the European Economic Area, unless requested by the customer in writing. Data transfers outside the EU or the EEA requested by customers will be carried out in compliance with the requirements specified in the EU General Data Protection Regulation. |
| **Practices related to the disclosure of data** | Data will be disclosed to the customer's auditor without prior authorisation for the purpose of implementing the agreement between the customer and the auditor. With regard to other partners of the customer, such as lawyers and consultants, authorisation will always be requested from the customer before disclosing any information.<br><br>When disclosing written materials, a certificate of disclosure will be drawn up, indicating the basic details of the materials, the party to whom they were disclosed and the time of disclosure. The certificate of disclosure will be stored in the customer's folders in case the disclosure needs to be proved later.<br><br>When disclosing digital materials, personal credentials will be created for the customer's partner, so that the partner can log in to the supplier's information system and access the disclosed data. The customer's request for creating credentials and granting access to the customer's data also means that the customer is consenting to the disclosure of the data to that particular partner.<br><br>Data will be disclosed to the tax authorities, pension insurance companies, insurance companies, trade union organisations, the Social Insurance Institution of Finland or employment pension funds without the customer's authorisation or consent when the disclosure is specified in legislation.<br><br>The processing of digital materials will be monitored by storing log data for the information systems and monitoring the data automatically or manually. If necessary, log data can also be used as evidence. |
| **Storage and erasure of data** | Talenom will erase personal data from its information systems after retaining it for five years following cessation of the customer relationship. After erasure from the operational information systems, the data will be automatically deleted from backups within six months. |

# DESCRIPTION OF REGISTER – PERSONAL DATA REGISTER FOR SPECIALIST SERVICES

| | |
|---|---|
| **Name of data register** | Personal Data Register for Specialist Services |
| **Applicable legislation** | General Data Protection Regulation (EU 679/2016) and National Data Protection legislation |
| **Last updated** | 31 July 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Otto-Pekka Huhtala<br>Tel: +358 (0)20 752 5276<br>Email: otto-pekka.huhtala@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | Personal data are stored and processed for the purpose of providing customers with Talenom's specialist services. |
| **Content of data register** | The following information can be stored on data subjects:<br>• Name and contact details<br>• Username and password<br>• Experience and skills profiles<br>• Calendar data and reservations |
| **Regular sources of data** | Personal data are mainly collected from the following sources:<br>• Data provided by the specialists themselves<br>• Basic data and contact details provided by Talenom |
| **Disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Talenom does not sell, rent or otherwise disclose personal data to other parties.<br><br>Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data will not be transferred outside the European Union or the European Economic Area. |
| **Practices related to the disclosure of data** | If data are disclosed to the authorities, a certificate of disclosure will be drawn up and stored in customer-specific folders. The data subject will always be informed of disclosure in advance, unless otherwise ordered by the authorities. |
| **Storage and erasure of data** | Talenom will erase the personal data of a specialist from the information systems immediately when the cooperation ends. After erasure from the operational information systems, the data will be automatically deleted from backups within six months. |

# DESCRIPTION OF REGISTER – VIDEO SURVEILLANCE IN OULU

| | |
|---|---|
| **Name of data register** | Video Surveillance in Oulu |
| **Applicable legislation** | General Data Protection Regulation (EU 679/2016) and National Data Protection legislation<br>Act on the Protection of Privacy in Working Life (759/2004)<br>Act on Equality between Women and Men (609/1986)<br>Occupational Safety and Health Act (738/2002) |
| **Last updated** | 31 July 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Johanna Rantasuo<br>Tel. +358 (0)20 752 5336<br>Email: johanna.rantasuo@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | Personal data are stored and processed for the purpose of ensuring the security and protecting the property of Talenom's office in Oulu, preventing crime and investigating offences (section 16 of the Act on the Protection of Privacy in Working Life, 759/2004). Talenom also has the right to use the data contained in the register for substantiating the grounds for the termination of an employment contract in situations specified in section 17, subsection 2(1–3) of the Act on the Protection of Privacy in Working Life (759/2004), for investigating and substantiating harassment as referred to in the Act on Equality between Women and Men (609/1986) or harassment and inappropriate conduct as referred to in the Occupational Safety and Health Act (738/2002), as well as for investigating an occupational accident or other dangerous or threatening situation as referred to in the Occupational Safety and Health Act. |
| **Content of data register** | The following information can be stored on data subjects:<br>• Images recorded on the premises and in the Oulu office areas using a continuously recording system. |
| **Regular sources of data** | Images provided by the cameras included in the video surveillance system of Talenom's Oulu office. |
| **Disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Talenom does not sell, rent or otherwise disclose personal data to other parties. Personal data contained in the register can, however, be disclosed to the authorities if crime is suspected.<br><br>Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data will not be transferred outside the European Union or the European Economic Area. |
| **Practices related to the disclosure of data** | If data are disclosed to the authorities, a certificate of disclosure will be drawn up and stored in the registers of the data protection officer. The data subject will always be informed of disclosure in advance, unless otherwise ordered by the authorities. |
| **Storage and erasure of data** | Images will be stored for six months. Images will be erased from the system automatically. |

# DESCRIPTION OF REGISTER – PHONE CALL RECORDINGS IN CUSTOMER SERVICE

| | |
|---|---|
| **Name of data register** | Phone Call Recordings in Customer Service |
| **Applicable legislation** | General Data Protection Regulation (EU 679/2016) and National Data Protection legislation |
| **Last updated** | 31 July 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Otto-Pekka Huhtala<br>Tel: +358 (0)20 752 5276<br>Email: otto-pekka.huhtala@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | Personal data are stored and processed for the purpose of providing customer service. Recording is conducted based on an agreement between Talenom and the customer, in accordance with Article 6 of the General Data Protection Regulation. Recorded phone calls will be used to prove what has happened and improve the quality of customer service. |
| **Content of data register** | The following information can be stored on data subjects:<br>• Name and contact details<br>• Organisation data<br>• Phone calls recorded when contact is established between the customer and the customer service centre |
| **Regular sources of data** | Personal data are collected when the customer calls Talenom's customer service centre or Talenom's specialists call the customer using Talenom's call management system. |
| **Disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Talenom does not sell, rent or otherwise disclose personal data to other parties.<br><br>Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data will not be transferred outside the European Union or the European Economic Area. |
| **Practices related to the disclosure of data** | If data are disclosed to the authorities, a certificate of disclosure will be drawn up and stored in the registers of the data protection officer. The data subject will always be informed of disclosure in advance, unless otherwise ordered by the authorities. |
| **Storage and erasure of data** | Recorded phone calls will be kept for six months, after which they will be erased from the information systems automatically. |

# DESCRIPTION OF REGISTER – RECRUITMENT REGISTER

| | |
|---|---|
| **Name of data register** | Recruitment Register |
| **Applicable legislation** | General Data Protection Regulation (EU 679/2016) and National Data Protection legislation |
| **Last updated** | 31 July 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Antti Aho<br>Tel. +358 (0)20 752 5405<br>Email: antti.aho@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | The purpose of the personal data register is to store and process job applications received by Talenom Plc. and the related data. Applicants can apply for a specific job or submit an open application. Applicants give their consent to adding their personal data to Talenom's recruitment database in accordance with Article 6 of the General Data Protection Regulation. |
| **Content of data register** | The following information can be stored on data subjects:<br>• Name and contact details<br>• Username and password<br>• Education and work experience<br>• Language skills<br>• Requested duties<br>• Experience and skills profiles<br>• Any additional information provided by the applicant |
| **Regular sources of data** | Data provided and stored in the system by the data subjects themselves. |
| **Disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Talenom does not sell, rent or otherwise disclose personal data to other parties.<br><br>Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data will not be transferred outside the European Union or the European Economic Area. |
| **Practices related to the disclosure of data** | If data are disclosed to the authorities, a certificate of disclosure will be drawn up and stored in customer-specific folders. The applicant will always be informed of disclosure in advance, unless otherwise ordered by the authorities. |
| **Storage and erasure of data** | Application data will be stored for six months after the application was submitted. |

# DESCRIPTION OF REGISTER – LIST OF SHAREHOLDERS

| | |
|---|---|
| **Name of data register** | List of Shareholders |
| **Applicable legislation** | Act on the Book-Entry System and Clearing Operations (348/2017), General Data Protection Regulation (EU 679/2016) and National Data Protection legislation |
| **Last updated** | 31 July 2018 |
| **Controller** | Talenom Plc.<br>Business ID: 2551454-2<br>Yrttipellontie 2<br>FI-90230 Oulu<br>Tel. +358 (0)207 525 000 (switchboard) |
| **Contact person** | Antti Aho<br>Tel. +358 (0)20 752 5405<br>Email: antti.aho@talenom.fi |
| **Data protection officer** | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| **Purpose of processing personal data** | Personal data is processed in accordance of Act on the Book-Entry System and Clearing Operations, for example for Talenom's shareholder follow-up, information about most influential shareholders and annual general meeting arrangements. Talenom's shares are part of electronic Book-Entry System and company's list of shareholders is maintained by Euroclear Finland. Talenom shareholder's personal data is processed in order to protect the vital interests of the shareholders and for compliance with legal obligations of stock market operations. Personal data of shareholders can be processed also in related activities that are not incompatible with the original intent of personal data processing. |
| **Content of data register** | The following information can be stored on data subjects:<br>• Shareholder's Name or Controller of the entry<br>• Social security number or other identification code<br>• Contact information, Payment information and Tax information<br>• Number of shares by category<br>• Central Securities Depository Contact managing Book-Entry Account<br>• Annual General Meetings participation list etc. personal data processing related to that<br>In addition to these, Talenom processes history data of shares and information about paid dividends.<br><br>For Annual General Meetings the information about shareholders of the company shares in Book-Entry System at reconciliation date of the meeting, list of shareholders indicating participation to the meeting and list of shareholders actually participating to the meeting, shareholders' assistants and deputies. Lists of Annual General Meetings contain for example following information:<br>• Shareholder name and Social Security Number<br>• Address, Phone Number and Email Address<br>• Account Number of Book-Entry Account, Number of Shares and Number of Votes<br>• Voting information<br>• Information about shareholders' Assistants and Deputies<br>Account Number of Book-Entry Account is only used in Euroclear Finland system for identification and it is not shared with Talenom. Talenom has right to review detailed voting information for verification of voting results. |
| **Regular sources of data** | Personal data are collected from Book-Entry System personal data register. Book-Entry System is maintained by Euroclear Finland and is responsible for the register management operations which are described in their Description of Data Protection. |

| | |
|---|---|
| **Disclosure of data** | Talenom can disclose personal data to any unit belonging to the Talenom Group. Talenom does not sell, rent or otherwise disclose personal data to other parties, unless it is necessary for securing Talenom's own legal obligations. In such cases Talenom verifies that the receiving party abides with the General Data Protection Regulation requirements through written agreement.<br><br>The following information can be viewed of every owner of a limited liability company on the public access terminal located at Euroclear Finland's customer service data terminal:<br>• name and address or home municipality of the owner<br>• date of birth<br>• nationality<br>• details on ownership<br>• number of waiting lists and reason for being on a waiting list<br>• information on any joint owners<br><br>The equivalent information can be viewed of every member of a cooperative on the customer terminal located at Euroclear Finland's customer service data terminal.<br><br>Euroclear Finland may disclose the data of the lists of ownership for direct marketing purposes or for marketing surveys and opinion polls, unless such disclosure has been forbidden by the data subject.<br><br>With regard to shares, share depositary receipts, pre-emption rights, options, warranties and bonds issued in the book-entry system and cooperative shares, Euroclear Finland will report the information necessary for taxation to the Tax Administration on book-entries incorporated in the book-entry systems, as well as their owners and yield recipients.<br><br>Personal Data processing in Book-Entry System happens in those countries that Euroclear Finland has informed, including India outside European Union. Euroclear Finland is responsible for contractual agreements on personal data processing with their sub-processors.<br><br>Talenom may be obliged to disclose personal data if required to do so under applicable law or regulations, or to meet a request by a judicial or administrative authority. |
| **Transfer of data outside the EU or the EEA** | Personal data acquired from Book-Entry System will not be transferred outside the European Union or the European Economic Area by Talenom. |
| **Practices related to the disclosure of data** | If data is disclosed to the authorities, a certificate of disclosure will be drawn up and stored in the customer specific repositories. |
| **Storage and erasure of data** | Personal Data in Book-Entry System, maintained by Euroclear Finland, will be maintained indefinitely. Personal Data regarding Talenom's annual general meetings are maintained at least the lifecycle of Talenom. |

# DESCRIPTION OF THE MEASURES FOR PROCESSING PERSONAL DATA

| | |
|---|---|
| Controller ("Customer") | Name<br>Customer |
| Processor ("Supplier") | Name<br>Talenom Plc. |
| | Address<br>Yrttipellontie 2, FI-90230 Oulu |
| | Other contact details (phone number, email address)<br>Tel. +358 (0)207 525 000 (switchboard) |
| Subcontractor's contact details | The Customer has given general power of using third party contractors for the Supplier. The Supplier will provide Customer a list of third party contractors upon request. |
| Data protection officer's contact details | Petteri Hyvönen<br>Tel. +358 (0)20 752 5560<br>Email: petteri.hyvonen@talenom.fi |
| Purpose of processing personal data | Personal data are stored and processed for the purpose of providing the Supplier's financial management services in accordance with the agreement between the Supplier and the Customer. Personal data are processed in order to meet the obligations provided by law and those related to official processing.<br><br>Personal data is processed in relation to:<br>• Customer's payroll and human resources administration<br>• Customer's accounting and receivables follow-up<br>• Limited company administration<br>• Association administration and invoicing<br>• Housing cooperation administration and invoicing<br>• Traffic Insurance, Health Insurance, Accident Insurance, Medicine Accident Insurance and Environmental Accident Insurance legislation benefits administration |
| Groups of data subjects and personal data groups | Customer's employees for payroll and human resources administration (HR)<br>Customer's person customers for accounting and following receivables (ACC)<br>Limited company stakeholders for limited company administration (LC)<br>Association members for association administration and invoicing (AA)<br>Housing cooperation members for housing cooperation administration and invoicing (HC)<br>Traffic Insurance, Health Insurance, Accident Insurance, Medicine Accident Insurance and Environmental Accident Insurance legislation benefits administration (IN)<br><br>The following personal data are processed:<br>• Name (HR, ACC, LC, AA, HC, IN)<br>• Address, phone number, email address (HR, ACC, LC, AA, HC, IN)<br>• Personal identity code (HR, LC, HC, IN)<br>• Account number (HR, ACC, LC, AA, HC, IN)<br>• Gender, mother tongue (HR)<br>• Employment contract data (HR)<br>• Salary data and salary bases (HR)<br>• Information on trade union membership fee (HR)<br>• Information on debt recovery enforcement (HR, ACC, LC, AA, HC, IN)<br>• Tax card, employment contract (HR)<br>• Hours entered, unit price (HR)<br>• Absences, holidays, doctor's certificates (HR) |
| Regular sources of data | The Customer adds the data of their staff members to the Supplier's digital services. Personal data can be loaded from digital materials provided by the customer. Personal data are collected in compliance with the terms and conditions of the Supplier's financial management |

| | |
|---|---|
| | systems.<br><br>In addition, personal data will be collected from the tax authorities, the Social Insurance Institution of Finland, trade union organisations, lending services, enforcement authorities and other parties who provide information that must be processed in payroll accounting.<br><br>Information about the devices of the users of the Supplier's digital products and online services will be collected automatically, using browser cookies or similar technologies, for the purpose of developing the digital products and improving customer service. |
| Groups of the recipients of personal data<br>- also those in third countries as well as international organisations (name) | The Supplier can disclose personal data within the limits allowed and provided by applicable legislation. Data contained in the register can be disclosed to the tax authorities, pension insurance companies, insurance companies, trade union organisations, the Social Insurance Institution of Finland or employment pension funds.<br><br>The Supplier has a statutory duty to disclose personal data to the authorities if they submit a lawful information request in writing.<br><br>Personal data will not be transferred outside the European Union or the European Economic Area, unless requested by the Customer in writing. Data transfers outside the EU or the EEA requested by customers will be carried out in compliance with the requirements specified in the EU General Data Protection Regulation. |
| Practices related to disclosing personal data | Data will be disclosed to the customer's auditor without prior authorisation for the purpose of implementing the agreement between the customer and the auditor. With regard to other partners of the customer, such as lawyers and consultants, authorisation will always be requested from the customer before disclosing any information.<br><br>When disclosing written materials, a certificate of disclosure will be drawn up, indicating the basic details of the materials, the party to whom they were disclosed and the time of disclosure. The certificate of disclosure will be stored in the customer's folders in case the disclosure needs to be proved later.<br><br>When disclosing digital materials, personal credentials will be created for the customer's partner, so that the partner can log in to the supplier's information system and access the disclosed data. The customer's request for creating credentials and granting access to the customer's data also means that the customer is consenting to the disclosure of the data to that particular partner.<br><br>Data will be disclosed to the tax authorities, pension insurance companies, insurance companies, trade union organisations, the Social Insurance Institution of Finland or employment pension funds without the customer's authorisation or consent when the disclosure is specified in legislation.<br><br>The processing of digital materials will be monitored by storing log data for the information systems and monitoring the data automatically or manually. If necessary, log data can also be used as evidence. |
| Technical and organisational security measures | Data contained in the data register that is processed electronically is protected by technical means: using firewalls and passwords, offering the Customer's employees two-step verification to the Supplier's information systems and using other technical means generally accepted in the security industry. Data transfer between the Customer and the Supplier is encrypted using Transport Layer Security (TLS) technology in the following services: Talenom Online, Talenom App, Mezo and Talenom Link. Data are backed up regularly and backups are stored in a separate location from the original data. |

| | |
|---|---|
| | The Supplier will protect the customer's data from unauthorised use and distribution. Only identified employees of the Supplier and the employees of companies operating on behalf of the Supplier have access to the data contained in the register, based on access rights granted to them. The access rights of users are monitored, and the user access management policy prohibits the creation of dangerous combinations of access rights. The creation of such combinations is monitored as part of access rights management. The access rights of the administrators of various systems, in particular, are reviewed regularly and removed when the user no longer needs them. The access rights of departing employees are deleted from all systems at the termination of employment.<br><br>Customer data are only processed by the employee assigned to that particular task. Processing personal data on any other grounds is prohibited, even if the employee has technical access to the data due to his or her role or for business reasons.<br><br>All Suppliers' employees, and any external persons operating on behalf of the Supplier, are bound to secrecy regarding all the Customer's financial management and personal data. The obligation of secrecy, including sanctions, is specified in the employment contracts of the Supplier's employees and the agreements concluded with third parties.<br><br>Employees who process the Customer's data receive regular training, a key part of which is the criteria for making data processing legitimate. The data security and data protection awareness of the Supplier's employees is maintained regularly by various means: By holding regular information sessions on the subject for all personnel and by organising an annual mandatory training course at the end of which employees must pass a test in order to complete the training.<br><br>The Supplier has a data security policy that every new employee must read through when joining the Supplier. Employees are informed of the existence and location of the data security policy, and reminded of its binding nature, at regular data security training sessions. The data security policy describes the general rules for data security and data protection that are binding on employees, including technical rules, data security processes, as well as practices and guidelines applicable to daily work.<br><br>Customer data are processed in information systems located in a data centre in Finland or in cloud services within the European Union. In the data centres located in Finland, the most important production systems have been duplicated and placed in two physically separate data centres so as to keep the data safe and secure the continuity of service under normal and emergency conditions. The data centres have certified security practices, access control and supervision in place maintained by the service provider.<br><br>Materials that are maintained manually are located on premises that have access control to prevent unauthorised access. The most important premises also have video surveillance, enabling the investigation and verification of possible breaches of physical security.<br><br>The Supplier will conduct internal and third-party assessments that cover both the technical security of critical information systems and the processes and guidelines related to administrative data security and data protection. |
| Planned erasure of data groups | The Supplier will erase the Customer's personal data from its information systems when the customer relationship ends. The data will be erased after five years following termination of the customer relationship. After erasure from the operational information systems, the data will be automatically deleted from backups within six months. |
| Rights of data subjects | The controller will describe the matters that are communicated to data subjects in a separate document created by the controller. |

| | |
|---|---|
| | In accordance with Articles 15 to 22 of the EU General Data Protection Regulation, data subjects have the following rights:<br>1. right of access to personal data<br>2. right to rectify the data<br>3. right to erase the data<br>4. right to restrict processing<br>5. right to data portability<br>These rights apply to personal data stored in Talenom's information systems. Certain rights of data subjects are restricted by other legislation, based on which Talenom has the right and obligation to legitimately refuse to rectify or erase data, restrict processing or transmit data from one system to another. One example of such legislation is the Accounting Act, which governs the storage of payroll documents, irrespective of the rights of data subjects specified in the General Data Protection Regulation.<br><br>If a data subject wishes to access or change his or her personal data contained in a personal data register owned by a customer of Talenom, the data subject must submit a request to access or change the data to the controller. The controller will then handle the request with the processor, i.e. Talenom. In such cases, the controller must submit a written request to the email address provided below.<br><br>The request to access or change data must specify the personal data that the data subject wants to access and provide the name of the data register concerned. The request must be submitted by email to: rekisteriseloste@talenom.fi. Data subjects can use their statutory right of access, provided by the General Data Protection Regulation, free of charge once a year. |
| Controller's instructions for processor | The Customer can draw up more detailed data processing instructions for the processor that the Supplier will keep in customer-specific folders and that will form part of the customer-specific payroll instructions. |
| Communicating personal data breaches | To the controller<br>The controller will be informed of a personal data breach without undue delay. The notification will describe the nature of the personal data breach and the measures taken, as provided by law.<br>To the data subject<br>The controller will inform the data subject of a personal data breach if the breach is likely to result in a high risk to the rights and freedoms of the data subject. The notification will describe the nature of the personal data breach and the measures taken, as provided by law.<br>To the supervisory authority<br>The data protection authorities will be informed of a personal data breach within 72 hours of its discovery if the breach is likely to result in a high risk to the rights and freedoms of the natural person. The notification will describe the nature of the personal data breach and the measures taken, as provided by law. |