PROCEDURES FOR ENSURING THE SECURITY OF THE PERSONAL INFORMATION OF CLIENTS OF ITPOINT OY

STATEMENT CONCERNING THE WAYS OF COMPLYING WITH THE EUROPEAN DATA PROTECTION REGULATION GDPR AT ITPONT OY

ITpoint Oy provides their clients with various ICT services which are produced, maintained, and developed with an emphasis on data protection. We provide most of our services from our own server rooms located in Finland.

We are responsible for the comprehensive data security of out clients' services, the conformity of our operations, and the continuity of the service production together with the client. We ensure the confidentiality, integrity, and availability of our client's service, regardless of whether the materials are specified as secret or confidential.

We employ various technological and administrative safety procedures to secure the data of our clients and to achieve the necessary protection level.

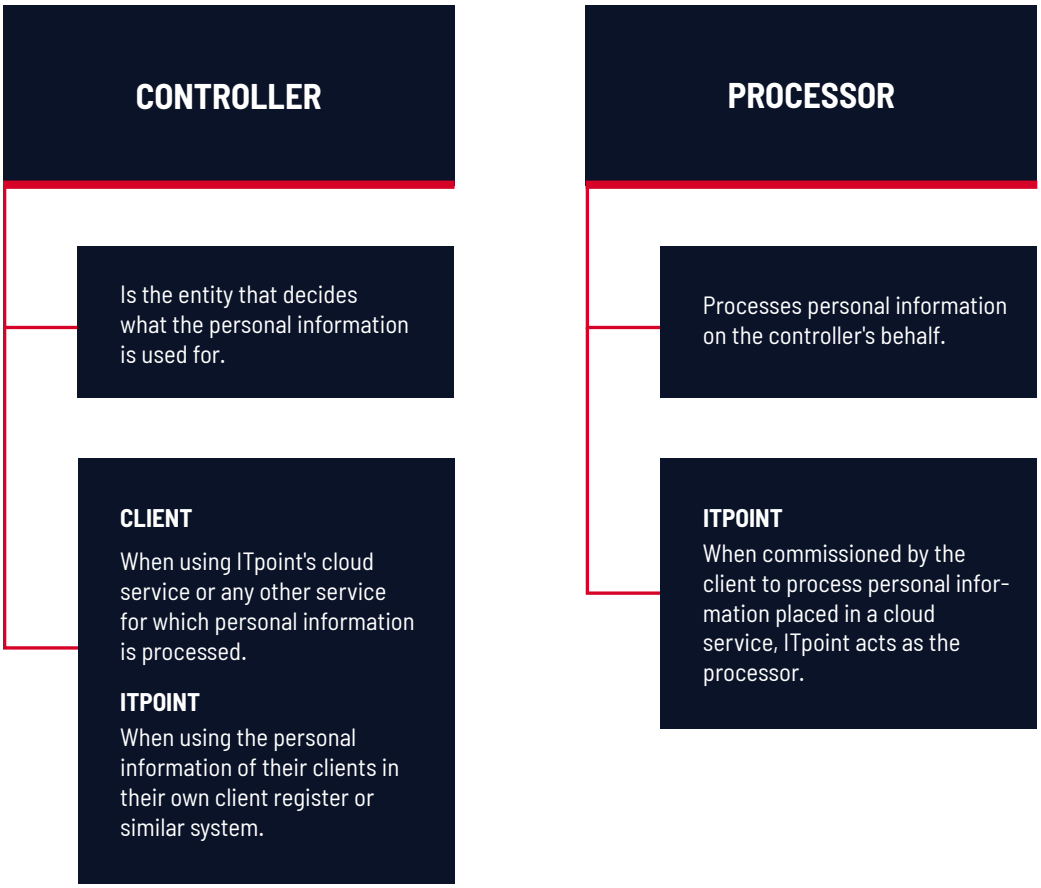
This document specifies the security arrangements we use and implement. We will sign a mutual service agreement with our clients, specifying in more detail the services at your disposal.

Should you have any questions about the details of this statement or the security of the service provided for you, we will be happy to answer them.

PROCEDURES FOR ENSURING THE SECURITY OF THE PERSONAL INFORMATION OF CLIENTS

ROLES RELATED TO DATA PROCESSING

If the service provided by ITpoint for the client includes processing of personal information, the client and ITpoint both shall be responsible for their own legal obligations as either the controller or data processor.



When processing the personal information they have placed in a cloud service provided by ITpoint, the client acts as the controller. If this information is processed by ITpoint by the client's commission, ITpoint is the processor and commits to acting in accordance with the law and all possible instructions issued by the client concerning said information.

ITpoint acts as the controller when processing the personal information of the client in their own systems, such as their own client register.

CLIENT COMPANY INFORMATION POSSESSED BY ITPOINT

The client shall own all data stored and transferred by them into ITpoint's services. Depending on the service, ITpoint's IT infrastructure may accumulate information concerning the client company's staff or the staff or clients of the client company,

for example when the client connects their personnel with the services or uses software administered by ITpoint. All stored personal information and its sensitivity vary according to service. As the client relationship ends, ITpoint shall close the data traffic, data system, data transfer, and remote use connections opened for the client and delete all data stored by the client in their systems.

PROCESSING OF PERSONAL INFORMATION OWNED BY THE CLIENT

Nature and purpose of the processing of personal data

Depending on the service offered to the client, the ITpoint staff who are responsible for technical maintenance may have access to the personal information of persons connected to the services, for example during helpdesk activities. ITpoint may process personal information for the purposes of maintaining and updating of the service and at the client's initiative for example to resolve a problem.

ITpoint's subcontractors

ITpoint may employ subcontractors in the provision of certain services. Should ITpoint employ subcontractors, the subcontractors are required to observe the same data protection principles.

DATA PROTECTION

When processing the client's data, ITpoint operates pursuant to the good data processing practices and data protection regulations required by the European data protection regulation.

ITpoint commits to keeping secret all confidential client information. ITpoint shall not use or utilise the client's materials for any purpose beyond that which is specified in the service agreement. The client's materials shall likewise not be handed over to third parties

Technical data protection

Data transfers requiring encryption shall be encrypted by means of appropriate encryption techniques unless otherwise agreed with the client.

ITpoint shall update and maintain the software and systems of their server centre regularly. Data protection updates for example are installed at least monthly. An effective and updated virus and malware protection mechanism is in place in the ITpoint server centre.

All of the data in the server centre are backed up at least daily and the copies stored in geographically separated locations.

Physical data protection

Our server centre is under 24-hour surveillance. Our centre incorporates electronic access controls and an alarm system that reports the status of the server room automatically.

The health of servers and other devices and software is monitored by a separate system which allows proactive reactions to possible problems and failures.

The uninterrupted power supply of the server centre is ensured by doubled power supply and auxiliary power systems.

Organisational security

The personnel of ITpoint has in their employment contracts signed a confidentiality clause applied to the data in the company's possession and to client data. The rights and powers of the personnel in the data systems used to provide the services are limited according to work tasks, and access to the systems is managed by targeted access rights. ITpoint's data and communications systems store data processing histories according to the needs of the service.

The daily operations of our personnel are guided by our joint corporate data protection guidelines. Data protection guidelines and practices are also included in the introduction of new employees. The personnel's knowledge and understanding of the requirements of the data protection regulation are developed and maintained by internal training and opportunities to take part in data protection training courses offered for example by our partners.

COMMUNICATIONS BETWEEN THE CLIENT AND ITPOINT

We shall notify the client of all relevant issues related to the use of the services, including service developments and changes. Our notifications are submitted for example via e-mail to the client's administrators and via our web pages and other electronic channels.

Despite the continuous development of the data protection of our services and the employed best practices, we are also prepared for communications related to possible data security violations. We monitor our environment actively and notify our clients without delay of any data security violations targeting their personal information, as regulated by the GDPR.