

## Privacy Policy

In the course of registration the Client/User gives the Service Provider information which falls into the category of protected personal data. The Service Provider can request such data in accordance with applicable laws of the Czech Republic, therefore obtained data are treated in compliance with the law (Act no 101/2000). Your personal data are collected, processed and stored only for the purpose of fulfilling our liabilities set out by the law in connection with execution of payment services ordered by our clients.

Collection and exchange of information is made by means of a secured server using SSL technology and a certificate with 128 bit coding system Thawte. The data collection server is also protected by an effective Firewall so your data are sufficiently secured against theft or misuse.

To make our communication safe and effective it is necessary to keep all contact information (e-mail, telephone) up to date. Therefore we request you in your own interest to keep your contact information in your User's Profile up to date. Change can be made after logging in directly on the page Profile. In case you decide to stop using our services, deactivate your Profile by rejecting your approval with our [General Business Terms](#). Please take into consideration the fact that according to the applicable laws we cannot completely delete all recorded information.

The User is responsible for protection of his/her logging in data needed for use of [FortiPay](#) service, as well as protection of his/her mobile phone against theft, misuse or unauthorised use by a third party and is fully liable for their misuse up to the moment when Fortissimo PI reports such a loss, theft or unauthorised use by a third party. In such case the user shall be fully liable for the incurred loss.

FORTISSIMO PI is obliged to block the Client's personalised payment facility as soon as a loss, theft or suspicion of unauthorised use is reported to FORTISSIMO PI in writing by the Client. FORTISSIMO PI shall be fully liable for loss arising from misuse only after the moment a loss, theft or unauthorised use of personalised protection facilities are reported.

Remember that we never require our Clients to disclose his/her password. Do not respond to false requests asking you to disclose your password for an alleged verification. If you forget your password, you can use our procedure [password renewal procedure](#). In case you have questions regarding applied security and protection of personal data, contact us at [info@devizy.cz](mailto:info@devizy.cz).