

## **Statement on Transaction Security and Confidentiality**

This Publica Security policy summary sets forth our general approach in the implementation and compliance of our internal security standards and issues providing payment services.

Buying book tokens on Publica.com platform is designed to be as simple as possible, while allowing maximum security and privacy for all your details.

Our secure server software (SSL) is the industry standard and is the best software available today for secure commerce transactions. It encrypts all of your personal information including credit card number, name and address so that it cannot be read as the information travels over the Internet.

We never store your credit card information. At no time do we store your credit card information on our server.

The encryption technologies we use are TLS and Amazon SES.

Publica.com ensures that you can purchase book tokens with complete confidence online. We have taken every possible measure to give you absolute security and confidence in your dealings with us.

Any data and information provided to us is encrypted using advanced technologies, and our website has security measures in place to protect against the loss, misuse and alteration of any data and information received by us. We continuously strive to safeguard the confidentiality of any such data and information and improve our security measures. We strive to use commercially reasonable means to protect your personal information.

Our Information System (IS) infrastructure is being constantly tested by our highly qualified security specialists to ensure it's best protection.

Publica is ensured for its secure business operations and always knows what to do, even on severe destructive events or force majeure regarding its strong administrative security control which includes developed BCP.

Security at Publica is a part of every employee's responsibilities. All our employees are encouraged to report on any security breach or potential security breach. Publica is supportive of an open environment for feedback and practices direct communication between staff of all levels and departments. Investigation and follow-up will be done by senior management regards all reported issues.

However we are hereby asking you as our client to perform the following actions also yourself to better protect the assets:

- keep your personalised credentials and payment instruments in secure manner;
- notify us immediately about your personalised credentials loss or compromise using the following e-mail address: [info@publica.com](mailto:info@publica.com)
- use up to date anti-malware software solutions