EVENT OPTIONS EU SECURITY POLICY

Event Options specialises in event RSVP and conference registration solutions. Owning hardware and software, we offer a flexible, pay-as-you-go pricing model using Evolve, a mobile-responsive RSVP and event check-in solution. At Event Options, we are dedicated to maintaining the security and confidentiality of our customers' data by adhering to data protection laws and maintaining a culture of security awareness through employee training.

This security policy outlines the measures that we have implemented to protect your information while using our conference registration solutions and associated services. By choosing to use our services, you agree to comply with this security policy and trust us to protect your data.

1. Data Collection and Usage

We collect and use personal data, including but not limited to *email addresses*, *phone numbers*, *names*, *organisation information*, and *addresses*, solely for the purpose of providing and developing our services. You agree to the collection and use of this information when registered to our service.

1.1. Data Collection
We collect your data through the following measures:
• Submission of forms on our websites or those provided by you.
• Participation in surveys.
• Posting comments or content on our social media pages or conference platform. • Direct communication with us, where you provide information.

1.1.1. Data Collected by Cookies
We use *Cookies* along with other tracking technologies to analyse data and enhance our service.
You have the option to set your browser to reject *Cookies*, but some features of our Service may not function properly without them.
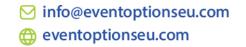
1.1.2. Payment-Related Information
We do not store any payment-related information in our databases, including *credit card numbers*, *bank account details*, or any other financial and payment-related information. Payment transactions are performed by third-party payment gateways that are secure and compliant, and no payment data is ever retained by Event Options. Currently, Event Options supports payment via following payment gateways:

• PayPal
• Paygate
• Payfast
• Worldpay
• Electronic Funds Transfer (EFT)

1.2. Personal Data Sharing and Retention
At Event Options, we do not disclose or sell your personal information to third parties for marketing purposes. However, we may share your data with some of our service providers, affiliates, business partners, sponsors, and other users to improve our services. In addition to this, we retain your personal information only to fulfil the purposes outlined in this policy. Unless otherwise required, your data in our system is deleted within 30 days of the event.

1.3. Security of Your Personal Data
While we are devoted to protecting your information, no method of transmission or storage is completely secure. But we take commercially reasonable steps to protect your information. In addition, we also try our best to protect your personal information by using up-to-date technology and by being compliant under applicable law.

1.4. Children's Privacy
Children under the age of 18 are not permitted to use our service. We do not gather personal information from children deliberately and if we come across such information, we will take appropriate action to remove it.

1.5. Your Choices, Rights, and Responsibilities
Event Options respects your ownership rights to your personal information. You have the following rights as the owner:

- You have a choice to request that we not contact you for marketing purposes. You can exercise this right at any time by selecting one of the several "opt-out" alternatives that we will always give you with every time we communicate with you. When you tell us not to, we will not send you promotional or event-related messages, nevertheless we will still need to send you service-related information.
- Links to third-party websites may be included in our services. While we make every effort to connect only to trustworthy sites, we have no control over their content or privacy practices. We advise you to read the Privacy Policies of these websites before providing any personal information.
- Your personally identifiable information may be transmitted to and processed in countries where our service providers are based. You consent to this transfer when you submit your information.
- At any time, you have the option to request clarification from us regarding the existence of any of your personal information in our possession.
- You have the right to request a copy of the personal information we have on record for you. We shall provide you with a copy of the information within a reasonable timeframe if we receive an authorised access request. You have the right to know the identity or categories of third parties to whom we have given your personal information. Such details will also be provided upon request.
- If you believe that any of the personal information we have on record for you is incomplete, misleading, incorrect, or excessive, you have the right to have it corrected or deleted. In compliance with current data protection rules, we will review your request and make any required modifications or deletions.

2. Infrastructure and Hosting

Event Options relies on Amazon Web Services (AWS), a highly secure and renowned cloud service provider, to host our event registration solutions and associated services. AWS's robust and scalable infrastructure adheres to strict security standards, ensuring the utmost protection for our clients' data.
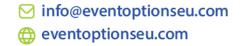
2.1. Access Control
AWS employs multiple layers of security controls, including physical, network, and data security measures, within their data centres. Access controls and surveillance systems are in place to prevent unauthorised access.

2.2. Encryption
Data transmitted between clients and our servers, as well as data at rest within our databases, is encrypted using industry- standard protocols like Transport Layer Security (TLS) and Advanced Encryption Standard (AES).

2.3. Compliance
AWS is committed to data security and privacy via compliance with the ISO/IEC 27001 standards.

3. Information Security

The Event Options system is built using *PHP Laravel* framework and ensures information security via following methods:

3.1. Authentication and Authorisation
Our robust and user-friendly authentication system with login throttling, CSRF protection, and password encryption, ensuring a secure and straightforward login experience. Additionally, our authorisation system provides fine-grained access controls, granting access to specific parts of your application only to authorised users, and safeguarding sensitive data and limiting actions to approved individuals.

3.2. Encryption
At Event Options, we have simplified the process of securing sensitive information, such as user credentials to ensure the confidentiality and protection of valuable data by using an inhouse API to encrypt and decrypt data effortlessly.

3.3. Secure Validation and Error Handling
We have implemented safe validation steps to prevent our system from security attacks such as SQL injection and cross-site scripting (XSS). Additionally, our error handling system is designed to send accurate error notifications only to authorised users, reducing the danger of data leakage.

3.4. Secure Third-Party Applications
This security policy outlines the security measures we have established to protect your information as you utilise our conference registration systems and related services. By using our services, you agree to follow our security policy and trust us to protect your data.

3.5. Database Security
Our databases are highly secured to prevent unauthorised access and data breaches.

3.6. File Permissions
We maintain correct file permissions to restrict access to sensitive files and directories.

3.7. Updated SSL Certificates
We regularly update and maintain secure SSL certificates to encrypt data exchanged between clients and our servers.

3.8. Daily Backups
We perform daily backups to ensure data integrity and provide a safety net against potential data loss.

4. Incident Response Management

- Event Options has established incident response procedures to handle security incidents effectively. The Incident Response Team will take appropriate actions to contain, mitigate, and recover from security incidents.
- Clients and users will be promptly notified via email in the event of planned system maintenance or unexpected downtime. The notification will include the reason, estimated downtime duration, and updates until normal operations are restored.

5. Secure Development Practices

- We follow a comprehensive Software Development Life Cycle (SDLC) methodology that governs the entire process of acquiring, developing, implementing, configuring, maintaining, modifying, and managing software components.
- To ensure the integrity and security of application source code, we use a version management mechanism. Access to the source code repository is reviewed on a regular basis and restricted to authorised employees.
- We have implemented a security-driven approach by conducting architecture reviews, open source scans, and dynamic application testing to ensure secure development practices.

6. Security Awareness

Event Options is committed to fostering a culture of security awareness among our employees. We conduct regular security training and education programs to ensure that all staff members are knowledgeable about potential risks and best security practices.

7. Policy Updates

This Security Policy may be updated periodically to reflect changes in our security practices and legal requirements. We will notify clients of any significant changes via email or through a notice on our website.

8. Contact Information

If you have any questions or concerns regarding our security policy, please contact us at info@eventoptionseu.com

This Security Policy outlines Event Options' commitment to maintaining a secure environment, protecting sensitive data, and responding effectively to security incidents. All employees and users are expected to adhere to this policy to ensure the highest level of security and data protection. Regular security audits and reviews will be conducted to identify potential vulnerabilities and enhance security measures as needed.