

Coalfire Systems, Inc. Privacy Program Overview



Commitment to Privacy

As a global cybersecurity leader, Coalfire Systems, Inc. ("Coalfire") prioritizes the safeguarding of client data. Our leadership is dedicated to upholding privacy regulations, ensuring transparency in our data handling practices, and fostering trust with our clients.



Commitment to Excellence

At Coalfire, we set high standards for safeguarding your data. Our employees undergo rigorous background checks and receive comprehensive privacy training upon hire and annually thereafter.

With a dedicated Privacy Team at the forefront, we proactively protect your personal data and prioritize transparency in our operations.

Rest assured, we comply with GDPR, CCPA, and other global privacy regulations to ensure your information remains secure and confidential.



Data Collecting and Processing

Our primary focus is on delivering services without unnecessary data collection or processing. When it's necessary, such as setting up employee information in our systems, we ensure it's limited to the basics. Importantly, we do not gather personal data from our clients' direct customers.

In instances where our cyber security services, like penetration testing, may encounter sensitive data, we handle it with utmost care and strictly adhere to our clients' agreements.

For further details, refer to our [Data Processing Agreement](#) (DPA) and [Privacy Policy](#).



Privacy Protection

We adhere to global privacy regulations and implement cross-border transfer mechanisms where necessary.

Both physically and electronically, we vigilantly monitor our offices and IT infrastructure to mitigate risks. Our comprehensive security measures include antivirus software, encryption

protocols, and detailed specifications outlined in the Technical Organizational Measures (TOMs) of our DPA.

Access to client data is strictly controlled through the principle of least privilege.

Our robust Business Continuity and Disaster Recovery plan ensured the resilience of our systems, and our Data Loss Prevention program consists of a multi-layered approach to monitoring the flow of information for data leaks.

When your contract with us ends, all services have concluded and data retention laws have been met, your data will be deleted promptly as defined by Coalfire's data retention requirements.



Data Breaches & Security Incidents

Coalfire has maintained a clean record with no data breaches in the last 5 years.

Nonetheless, we are prepared with a robust Incident Response Plan to swiftly address any unforeseen circumstances. In the unlikely event of a breach, we are committed to promptly notifying affected parties, with detailed procedures outlined in our DPA.



Third-Party Risk

Management

We prioritize meticulous management of third-party risks to ensure the integrity of our services. Our list of sub-processors is transparently provided in Annex III of our DPA, with notifications promptly issued for any changes.

Additionally, each sub-processor undergoes thorough scrutiny by our Chief Information Security Officer (CISO) to guarantee compliance and mitigate potential risks.



Additional Information

Typically, Coalfire is the data processor when you engage with us.

Our commitment to security is underscored by our certifications in SOC and ISO standards.

Any new offerings undergo a comprehensive privacy review via our Go-to-Market review process.

You can access the list of sub-processors in the DPA to gain insight into where data is stored.



Policies/Practices

Coalfire's Implemented

Coalfire has implemented a comprehensive set of policies and practices to uphold privacy and security standards. These include the Privacy Policy, DPA, and adherence to ISO/IEC 27001:2013 and ISO/IEC 27701:2019 certifications.

Our proactive approach involves monitoring and responding to the regulatory environment. We conduct Data Protection Impact Assessments (DPIA), Records of Processing Activities (ROPA), and respond to Data Subject Access Requests (DSAR) to mitigate risks.

Additionally, we enforce policies such as Data Classification & Handling, Data Retention/Destruction, and Access Management. While encryption is primarily a security measure, it contributes to privacy protection.

Importantly, all policies undergo regular review, ensuring continued alignment with evolving privacy and security best practices.



Contact Us

Questions? Reach out to us at privacy@coalfire.com or visit our [Privacy Policy](#) for more information.

For questions about our security protocols, reach out to Compliance@coalfire.com.

Note: this overview is provided as a courtesy, for more information contact us directly.

Copyright © 2024 Coalfire Systems, Inc.

All rights reserved. Coalfire and the Coalfire Logo are trademarks or registered trademarks of Coalfire Systems, Inc. or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners.