This Data Protection Addendum ("DPA") hereby amends the Services Agreement available at https://www.coalfire.com/agreements/sa or such other agreement entered into by you as a company or individual ("Client") and Coalfire Systems, Inc. or its Subsidiaries (collectively, "Coalfire") as well as the ordering documentation that governs the provision of products and services by Coalfire to Client (collectively in each case, the "Agreement"). This DPA only applies when Personal Data is processed by Coalfire pursuant to the Agreement. This DPA is incorporated into and forms part of, and is subject to the terms and conditions of, the Agreement. If an Affiliate of Client has executed an order with Coalfire but is not the original signatory to the Agreement, this DPA is an addendum to and forms part of such order. Capitalized terms used in this DPA will have the meanings set forth in Exhibit A.

1. **COMPLIANCE WITH LAWS**. Each of Client and Coalfire will comply with all applicable Data Protection Laws in the performance of its obligations under this DPA, including the Processing of Personal Data. Client acknowledges that Coalfire is not responsible for determining the requirements of Data Protection Laws applicable to Client's business.

2. **PROCESSING OF PERSONAL DATA**. In connection with the Services that Coalfire provides to Client pursuant to the Agreement, Coalfire may Process, on behalf of Client, some Client data that contains Personal Data relating to Data Subjects. Coalfire and Client agree that with regard to the Processing of Personal Data under Data Protection Laws, Client is the Controller and Coalfire is the Service Provider or Processor.

3. **CLIENT INSTRUCTIONS**. Coalfire will only Process Personal Data on behalf of and in accordance with Client's Documented Instructions. Client's instructions for the Processing of Personal Data by Coalfire shall at all times comply with applicable Data Protection Laws and Client shall ensure that Coalfire's Processing of Personal Data in accordance with Client's instructions will not cause Coalfire to violate any applicable Data Protection Laws. Coalfire is not required to comply with or observe Client's instructions if, in its reasonable discretion, such instructions would violate any Data Protection Laws. If Coalfire becomes aware that the Documented Instructions are in conflict with applicable Data Protection Laws, Coalfire will suspend any processing that is in violation of the law and promptly notify Client.

4. **CLIENT'S RESPONSIBILITY**. Client recognizes that Coalfire cannot verify (i) the residency of each Data Subject; nor (ii) the aspects of Personal Data that are provided to Coalfire by Client. Client is responsible for ensuring that all Personal Data may be Processed by Coalfire in compliance with Data Protection Laws, and Coalfire will provide all reasonably necessary information to Client to allow Client to make such determination upon Client's written request. Client is responsible for ensuring that it has, and will continue to have, the right to transfer, or provide access to, Personal Data to Coalfire for Processing. Client will ensure that it has obtained and will obtain all necessary consents, and has given and will give all necessary notices, for the Processing of Personal Data by Coalfire in accordance with the Agreement.

5. **STORAGE AND ACCESS TO PERSONAL DATA**. All Personal Data is stored by Coalfire or its Sub-processors in the United States for operational purposes. Coalfire will ensure that access to Personal Data is restricted to only those personnel who have a need to know in order for Coalfire to perform its obligations under the Agreement and this DPA. Coalfire personnel engaged in the Processing of Personal Data will be informed of the confidential nature of the Personal Data and be bound in writing by obligations of confidentiality sufficient to protect Personal Data in accordance with the terms of this DPA.

6. **SUB-PROCESSING**.

6.1 Authorized Sub-processors. Client agrees that Coalfire may use Sub-processors to fulfill its contractual obligations under the Agreement, including any Service Order and this DPA. Sub-processors may include Subsidiaries of Coalfire. Client provides general written authorization to Coalfire to engage Sub-processors to perform the Services. The current list of those Sub-processors that are engaged by Coalfire to carry out processing activities on Personal Data is available at https://coalfire.com/legal/sub-processor-list. Coalfire will notify Client of any new Sub-processor that it engages to carry out processing activities on Personal Data by adding them to this list. Client will have ten (10) business days to reasonably object that this Sub-processor will cause Client to be in violation of the Data Protection Laws. If Client does not object during this time, Client is deemed to have waived its right to object and to have consented to the new Sub-processor.

6.2 Sub-processor Obligations. With respect to each authorized Sub-processor:

(a) Coalfire will enter into a written agreement with the Sub-processor that imposes obligations to protect Personal Data in accordance with the Data Protection Laws; and

(b) Coalfire will be liable for the performance of the Sub-processor to the same extent that Coalfire would be liable if Processing Personal Data itself.

7. **DATA SUBJECT RIGHTS**. Taking into account the nature of the Processing, Coalfire will assist Client by implementing appropriate technical and organizational measures, to the extent that this is possible, for the fulfillment of Client's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws. Coalfire will promptly notify Client if it receives a request from a Data Subject under any Data Protection Law with respect to the Personal Data, and Coalfire will not respond to that request except on the instructions of Client or as required by applicable law. Coalfire will respond to that request if Client does not provide instructions or respond within the applicable timeline.

8. **SECURITY OF DATA PROCESSING**. Coalfire has implemented and will maintain appropriate technical and organizational measures to protect Personal Data against accidental and unauthorized disclosure of or access to Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The technical and organizational measures implemented by Coalfire are set forth in Coalfire's Risk Assurance Program, available upon Client's request and subject to the confidentiality provisions of the Agreement.

9. **PERSONAL DATA BREACHES**

9.1 **NOTIFICATION**. Coalfire will notify Client without undue delay upon becoming aware of a Personal Data Breach. Coalfire will provide Client with sufficient information to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws, subject to the availability of such information and any restrictions on the disclosure of such information. Notwithstanding anything to the contrary in the Agreement, Coalfire may notify Client of a Personal Data Breach via email.

9.2 **ASSISTANCE**. Coalfire will cooperate with Client and take reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each Personal Data Breach. Coalfire's obligation to report or respond to a Personal Data Breach under this Section 9 is not and will not be construed as an acknowledgement by Coalfire of any fault or liability of Coalfire with respect to the Personal Data Breach.

10. **DELETION OF PERSONAL DATA**. Following expiration or termination of the Agreement, or upon Client's request, Coalfire will delete any Personal Data in Coalfire's possession, where it is able to do so. However, Coalfire may retain Personal Data to the extent Coalfire is required to do so by applicable law or a Certifying Agency. The terms of this DPA will continue to apply to such Personal Data.

11. **SECURITY AUDITS**. Coalfire uses both internal and external auditors to verify the adequacy of its security measures with respect to its Processing of Personal Data. Upon Client's request, and provided that the parties have an adequate confidentiality obligations in place, Coalfire will make available to Client its most current System and Organization Controls (SOC) 2 Type II Report and/or summary of its most recent relevant audit report and/or other documentation reasonably required by Client to verify Coalfire's compliance with this DPA.

12. **GDPR**. This Section 12 applies only to Personal Data subject to GDPR:

12.1 **DETAILS OF DATA PROCESSING**. Client will only provide or disclose to Coalfire that Personal Data described below. If Client wants to provide or disclose any other Personal Data to Coalfire or wants Coalfire to process any Personal Data outside the scope of the Documented Instructions, Client and Coalfire must agree in writing to a modification of the Personal Data and/or

Documented Instructions. If Coalfire declines to agree to the requested modification, Client may terminate the Agreement in accordance with its terms.

Subject Matter	Duration	Purpose	Nature of the Processing	Type of Personal Data	Categories of Data Subjects
Services purchased by Client from time to time	The last to occur of: (a) expiration or termination of the Agreement, including any form of ordering document; (c) any applicable retention periods in the Agreement; or (d) until the Personal Data being processed is no longer necessary for the purposes of either party performing its obligations under the Agreement	The delivery of Services purchased by Client from time to time. When Client engages Coalfire to provide services, the services and deliverables that Client elects to purchase from Coalfire will be defined in a written agreement.	Collection, review, use, storage and such other Services purchased by Client from time to time	Name, title and business contact information	Client's employees and contractors – points of contact
			Collection, review, use, storage and such other Services purchased by Client from time to time	Name, title, business contact information, education, experience and IP addresses	Client's employees and contractors – personnel responsible for fulfilling obligations under applicable certifications
			Incidental observation and temporary storage	Personal data as defined in the GDPR	Client's employees, contractors, customers, end users and/or suppliers

12.2 **CONFIDENTIALITY OF PERSONAL DATA**. Coalfire will require that any individual authorized to process Personal Data commits to safeguarding Personal Data consistent with Coalfire's confidentiality obligations under the Agreement. Client acknowledges that Coalfire may share Personal Data with its consultants, auditors, or other third parties as necessary for fulfilling its responsibilities under this DPA, the Agreement, or delivering Services to Client.

(a) Governmental Bodies. If a governmental body sends Coalfire a demand for Personal Data, Coalfire will attempt to redirect the governmental body to request that data directly from Client. As part of this effort, Coalfire may provide Client's basic contact information to the governmental body. If compelled to disclose Personal Data to a governmental body, Coalfire will give Client reasonable notice of the demand to allow Client to seek a protective order or other appropriate remedy unless Coalfire is legally prohibited from doing so.

(b) Certifying Agencies. If a Certifying Agency sends Coalfire a demand for Personal Data, Coalfire will disclose such data in accordance with the requirements of the guidelines of Certifying Agency, which guidelines Client agrees to by seeking certification from the Certifying Agency.

12.3 **SECURITY OF DATA PROCESSING**. The technical and organizational security measures implemented by Coalfire, include, as appropriate, the measures referred to in Article 32(1) of the GDPR.

12.4 **PRIVACY IMPACT ASSESSMENT AND PRIOR CONSULTATION.** Taking into account the nature of the Services and the information available to Coalfire, Coalfire will assist Client in complying with Client's obligations in respect of data protection impact assessments and prior consultation pursuant to Articles 35 and 36 of the GDPR, by providing the information Coalfire makes available under Section 11, Security Audits.

12.5 **CLIENT AUDITS**. Client agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing Coalfire to carry out the audit described in Section 11, Security Audits. If Client wishes to change this instruction regarding the audit, then Client has the right to request a change to this instruction by sending Coalfire written notice as provided for in the Agreement. If Coalfire declines to follow any instruction requested by Client regarding audits or inspections, Client is entitled to terminate the Agreement in accordance with the terms of the Agreement.

12.6 **TRANSFERS AND EXPORTS OF PERSONAL DATA.**

(a) **STANDARD CONTRACTUAL CLAUSES**. Coalfire may transfer and process Personal Data to and in other locations around the world where Coalfire or its Sub-processors operate, as necessary to provide the Services. Where Personal Data is transferred from the EEA, United Kingdom or Switzerland to Coalfire or its Sub-processors (including Subsidiaries of Coalfire) in a country that is not recognized by the European Commission, UK Information Commission, or the Swiss Data Protection Authority as providing an adequate level of protection for Personal Data, the Standard Contractual Clauses will apply. If there is any conflict between the provisions in the body of this DPA and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses will take precedence with respect to the transfer of Personal Data outside the EEA.

(b) **CLARIFICATIONS**. The Standard Contractual Clauses are subject to the following clarifications:

(i) Clause 8. For the purposes of Clause 8 of the Standard Contractual Clauses, the reference to "instructions" means the Documented Instructions.

(ii) Clauses 8 8 and 13(b). The audits described in Clause 8.9 and Clause 13(b) of the Standard Contractual Clauses shall be carried out in accordance with the provisions of Section 11, Security Audits.

(iii) Clause 9(a). Pursuant to Clause 9(a) of the Standard Contractual Clauses, Client acknowledges and agrees that Coalfire may engage Sub-processors in connection with the provision of the Services. Coalfire will make available to Client an up-to-date list of all Sub-processors used for the processing of Personal Data in accordance with the provisions of Section 6.1, Authorized Sub-processors. Client acknowledges and expressly agrees that Coalfire may engage new Sub-processors in accordance with the provisions of Section 6.1, Authorized Sub-processors.

(iv) Clause 9(c). Pursuant to Clause 9(c) in the Standard Contractual Clauses, Coalfire will provide copies of the Sub-processor agreements only upon reasonable request by Client. To the extent necessary to protect business secrets or other confidential information, including personal data, Coalfire may redact the text of the agreement prior to sharing a copy.

(v) Clause 14(d). For purposes of Clause 14(d), termination of the provision of data processing services will not occur until the expiration of any applicable data retention requirement, and a certification of deletion of Personal Data will be provided by Coalfire to the Client only upon Client's request.

13. **CCPA**. This Section 13 applies only to Personal Data subject to CCPA. The terms "Business," "Business Purpose", "Commercial Purposes", "Consumer", "Sell", "Service Provider" and "Verifiable Consumer Requests" have the same meaning as in the CCPA.

13.1 Roles. Client is a Business and appoints Coalfire as a Service Provider.

13.2 Processing and Sharing. Coalfire will process Client Personal Data only for business purposes necessary to provide Services and may share business contact information with subcontractors, affiliates, and other service providers for service delivery, security monitoring, compliance, and customer relationship management purposes, subject to appropriate confidentiality protections.

13.3 Consumer Requests. Coalfire will promptly notify Client of consumer rights requests and cooperate in Client's response.

13.4 Compliance. Coalfire will maintain appropriate privacy protections, will not sell Client Personal Data, and will not retain data longer than necessary to provide Services or as required by law.

14. **GENERAL**

14.1 **DATA PRIVACY OFFICER**. Coalfire's data privacy officer can be contacted at privacy@coalfire.com.

14.2 **EFFECT ON THE AGREEMENT.** Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the provisions of this DPA and the Agreement, the provisions of this DPA will govern for the subject matter for this DPA only.

14.3 **TERM**. The term of this DPA will continue until the deletion of all Personal Data by Coalfire as described in this DPA.

EXHIBIT A
DEFINITIONS

"Affiliate" means an entity controlling, controlled by or under common control with a party.

"CCPA" means the California Consumer Privacy Act as amended by the California Privacy Rights Act, Cal. Civ. Code § 1798.100 *et seq.,*

"Certifying Agency" means an agency or organization from which Client is seeking certification, including, without limitation, the Payment Card Industry Security Standards Council (PCI SSC), the Federal Risk and Authorization Management Program (FedRAMP) and the Health Information Trust Alliance (HITRUST).

"Consumer Rights Request" means a request made by a Consumer to exercise the rights granted to Consumers under the CCPA.

"Controller" means the entity that determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws" means data protection and privacy laws throughout the world to the extent that they apply to the processing performed by Coalfire pursuant to the Agreement. Data Protection Laws may include the GDPR and CCPA.

"Data Subject" means the individual to which the Personal Data relates.

"Documented Instructions" means this DPA and the Agreement, as same may be amended by the parties in writing, and Client's use of any features and functionality in the Services.

"EEA" means the European Economic Area.

"GDPR" means General Data Protection Regulation 2016/679 and its implementation by member countries in the European Union and EEA and the UK's Data Protection Act 2018.

"NDA" means a non-disclosure or confidentiality agreement entered into by Client and Coalfire that covers the exchange of confidential information.

"Personal Data" means that any information relating to an identified or identifiable natural person as defined under applicable Data Protection Laws.

"Personal Data Breach" means an incident resulting in the unauthorized disclosure of or access to Personal Data (excluding pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incident where there is no unauthorized disclosure of or access to Personal Data).

"Process" or "Processing" means any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity that Processes Personal Data on behalf of the Controller.

"Risk Assurance Program" means Coalfire's Risk Assurance Program, which sets forth the security measures implemented by Coalfire, as same may be updated by Coalfire from time to time.

"Services" means those services and/or products provided by Coalfire to Client.

"Standard Contractual Clauses" means Exhibit B, attached to and forming part of this DPA pursuant to the European Commission Implementing Decision of June 4, 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries under pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"Sub-processor" means any Processor engaged by Coalfire to Process Personal Data.

"Subsidiaries" means those entities controlled by Coalfire Systems, Inc., where control means possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting stock or otherwise.

EXHIBIT B

EU and UK STANDARD CONTRACTUAL CLAUSES

For the purposes of Regulation (EU) 2016/679 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Client" in the DPA
(the "**data exporter**")

and

Coalfire Systems, Inc.
330 N Wabash Ave, Suite 1430, Chicago, IL, 60611, USA

(the "**data importer"**)

each a "party"; together "the parties",

HAVE AGREED on the following contractual clauses (the "Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex I.B.

Schedule I – Standard Contractual Clauses

1.1 To the extent legally required, the signatories to the Agreement are deemed to have signed the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=e (the "2021 Standard Contractual Clauses"), which form part of this DPA and will be deemed completed as follows:

1.1.1 Module 2 of the 2021 Standard Contractual Clauses applies to transfers of Personal Data from Client to Coalfire.

1.1.2 Clause 7 of Module 2 (the optional docking clause) is not included;

1.1.3 Under Clause 9 of Module 2 (Use of sub-processors). the parties select Option 2 (general authorization). The contents of Annex III (the list of sub-processors already authorized by Customer) are attached hereto as Schedule 3 to this DPA;

1.1.4 Under Clause 11 of Modules 2 (Redress). the optional language requiring that data subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

1.1.5 Under Clause 17 of Modules 2 (Governing law). the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the laws of Ireland;

1.1.6 Under Clause 18 of Modules 2 (Choice of forum and jurisdiction). the parties select the courts of Ireland.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: … As described in the Agreement.

Address: … As described in the Agreement

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: … Activities and processing operations are defined in Section 12 of the DPA

Signature and date: …

Role (controller/processor): controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: As described in the Agreement.

Address: As described in the Agreement.

Contact person's name, position and contact details:Privacy@coalfire.com

Activities relevant to the data transferred under these Clauses: Activities and processing operations are defined in Section 12 of the DPA

Signature and date:

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set out in Exhibit A and Section 12, GDPR of the DPA

Categories of personal data transferred

As set out in Exhibit A and Section 12, GDPR of the DPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None anticipated

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuously, for the length of the Agreement between the parties.

Nature of the processing

Personal data will be processed for purposes of fulfilling Coalfire's obligations to Client under the Agreement and the DPA.

Purpose(s) of the data transfer and further processing

For Coalfire to provide services to Client pursuant to the agreement between the parties.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data shall be retained for the length of time necessary to provide the Services under the Agreement, or as otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Coalfire's sub-processors may process personal data to assist Client in providing the Services pursuant to the Agreement for as long as needed in order for Coalfire to provide the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13…Ireland

[End of Annex I]

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data Security and Access Control (Management, Storage, and Transmission)

Coalfire maintains a cryptographic controls and data classification/handling program to protect all client documentation while entrusted to the Coalfire Assessment System. All "Sensitive and Proprietary –Customer Information" must be protected via strong cryptography while in transport and storage. Our cryptographic controls program leverages AES-256 ciphers to protect information while in transport via TLS 1.2+ and AES-256 encryption for documents in storage.

Coalfire laptops or other remote PCs that are used to remotely connect to Coalfire networks must employ encrypted volumes to protect the remote storage of any Coalfire–Sensitive and Proprietary information. Access to Coalfire systems is available for authorized users over the Internet via our secure VPN connection.

Physical Security

Coalfire has implemented physical security controls at its offices, datacenters/closets, and work areas commensurate with the risk to our people and of the information assets stored, processed, or transmitted within those areas. This includes the appropriate environmental and physical safeguards necessary to protect Coalfire assets from unauthorized access, theft, damage, or destruction.

Documentation

Coalfire will validate that the necessary documentation is in place between Coalfire and its clients where Coalfire processes personal or sensitive data covered by the GDPR, including, but not limited to DPAs,NDAs, SCCs and, where applicable, Sub-processor agreements.

Privacy by Design: Testing, Assessment, and Evaluation

Coalfire employees will embed privacy into the design and architecture of Coalfire's IT systems and business practices, to include password protocols and protections, multi-factor authentication and other measures to ensure the security and integrity of data. For authentication on data processing systems, secure passwords are used that have sufficient length and are robust against the known forms of dictionary and logical attacks. Passwords must be changed on a regular schedule and systems are locked where password updates have not occurred. Where technically appropriate, the use of multi-factor authentication is enforced.

All employees must attend both new hire and regular basic privacy and data security training as well as and participation in such training is recorded. Employees are also required to regularly certify that they will comply with Coalfire's ethical business conduct, confidentiality and security policies.

User Access Management

Coalfire only grants and provides the least amount of access to data on a "business need-to-know" basis. Users are granted the minimum amount of access required to successfully fulfill their job requirements. All access granting systems employed by Coalfire leverage "deny all" principles. User accounts are personal to all employees and not shared. All user activities, including logon attempts to IT systems are recorded and maintained.

Media Handling

Coalfire will protect the information it owns or possesses based on the nature of the information and the risk exposure to the organization, and its customers. Coalfire will ensure that appropriate safeguards are in place to protect our information from inappropriate or undesired access, disclosure, or destruction. The degree of protection provided to information must correlate directly with the inherent risk of this information and will observe all relevant laws and regulations. These safeguards must be implemented throughout the lifecycle of information, including creation, handling, processing, retention, and disposal.

Controls and Validation

In addition to maintaining certifications that are independently audited as part of a comprehensive audit program. Coalfire employs an internal audit team that regularly conducts IT security audits, data protection audits and ensures that compliance and regulatory frameworks are being followed. IT and IT security governance processes are subject to the controls outlined in the SOC2 "Assessment Environment" and Coalfire's written information security plan. A full description of the security controls is outlined in the SOC2 report. Coalfire is audited externally and adheres to ISO 27001, ISO 27701, and SOC 2 Type 2 controls.

Sub-processors

Coalfire maintains a listing of all sub-processors utilized in the provision of its services. Sub-processor agreements are required and maintained with appropriate flow-downs to match client requirements. Sub-processors are fully vetted and regularly monitored to ensure that sub-processor systems and policies meet Coalfire standards and requirements.

Risk Management

Coalfire has assessed and will regularly update risks related to the processing of personal data covered by the GDPR and create and maintain an action plan to mitigate identified risks.

Threat and Vulnerability Management

Coalfire maintains a full vulnerability detection and remediation program, which includes weekly scans and annual penetration tests, as well as annual code review. Coalfire leverages Carbon Black Defense, a next-generation AV/anti-malware tool. All internal networks are monitored by IDS at key points. Coalfire maintains a full monitoring program that includes central event aggregation and alerting within our SIEM, as well as cloud service monitoring within our CASB. Logging on processes are subject to the controls outlined in the SOC2 "Assessment Environment" and Coalfire's written information security plan. A full description of the security controls is outlined in Coalfire's SOC2 report.

System Configuration Management

Coalfire maintains a strict systems configuration program that requires systems to be built against industry best-practice security benchmarks. This program includes changing system defaults, removal of uncessary software and programs, and configuring security settings to a hardened state. This program is required for all servers, workstations, and mobile devices participating in the corporate information system.

Security Incidents and Event Logs

Coalfire maintains an incident management program that incorporates event monitoring solutions, user-reported events, and other security events. The security incident response plan (SIRP) is tested annually. In the event of an incident impacting the customer, the Coalfire procedure is to notify either a contractually designated entity or the primary POC for contracted work. Notification occurs within 3 business days of confirmation of the incident.

Data Minimization

Coalfire only collects the minimum amount of data required to fulfill its business obligations with the various organizations with which it does business. These practices are included in Coalfire's Privacy Policy. In addition, Coalfire stores only the minimum amount of data in each of its data centers. Storage repositories must also be approved by Coalfire management before they are secured and utilized.

Data Retention and Restoration

Data backups of databases and operating system images are taken to the extent required or otherwise appropriate with the aim of preventing the loss of personal data in the event of a technical malfunction or human error. Backups are performed for servers in productive operation and the recovery of data backups is tested. Processes or procedures for handling disruptions to IT systems and for restoring systems after a disruption have been established as part of Coalfire's business continuity management protocols.

Retention period is subject to Coalfire's written and technically enforced data retention schedule as well as retention schedules required in our client contracts and applicable law. Data retention for file-based project artifacts occurs according to the documented

data retention schedule in the Information Security Plan. Conversely, schedules for the return, erasure or destruction of data as required contractually or by law are recorded, maintained and strictly enforced. Guidance from oversight bodies on retention of data are strictly enforced.

Accountability

Coalfire has adopted and implemented data protection policies, recorded and maintained documentation of processing activities and incidents, employed qualified and skilled personnel and adopted a range of programs in order to ensure accountability of Coalfire's technical and operational requirements, including:

- Leadership and oversight: Coalfire employs its Chief Information Security Officer, whose team is responsible to protect Coalfire's IT environment and to create, update, test and oversee its programs, policies and procedures.
- Training and awareness: All Coalfire employees must attend both new hire and regular basic privacy and data security training as well as and participation in such training is recorded. Employees are also required to regularly certify that they will comply with Coalfire's ethical business conduct, confidentiality and security policies.
- Adopted Plans: Information Security Plan; Security Incident Response Plan plus policies related to information security, ethics, and employee and vendor conduct.

Data Portability and Ensuring Erasure

It is rare, if ever, that requests to port data are received by Coalfire, save for its transmission of data to its Sub-processors, who are all bound by contract and are regularly monitored by Compliance. Coalfire maintains a Data Disposition Policy and Standard that outlines the secure deletion and destruction of data. Coalfire's Compliance Team requests deletion/destruction/erasure of data from a particular file, based upon a schedule maintained for each client, vendor or related party. Once the IT team receives this request, appropriate action is taken, and confirmed both by the IT team and Compliance.

[End of Annex II]

Annex III: UK Addendum to the EU Standard Contractual Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set forth in Annex I
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

[End of Annex III]