DATA PROCESSING ADDENDUM

1. INTRODUCTION

1.1. This Data Processing Addendum ("**DPA**") sets forth the terms and conditions relating to the privacy, confidentiality, security and protection of Protected Data (as defined below) to be processed as part of the (a) provision of the Services by Cognism and (b) receipt and use of the Services by the Customer pursuant to the services agreement entered into between Cognism and the Customer (the "**Agreement**").

1.2. In the event of any conflict or inconsistency between the terms of this DPA and any other terms in the Agreement, this DPA shall prevail.

2. DEFINITIONS

2.1. Capitalized terms used but not defined in this DPA will have the meanings provided in the Agreement. The following terms shall have the meanings set out below:

"Adequate Jurisdiction"	means (a) in case of transfers from the EU: (i) a country within the European Economic Area ("**EEA**"); or (ii) a country, territory or sector within a country which is and continues to be the subject of a valid adequacy decision by the European Commission ("**EC**"); or (b) in the case of transfers from the UK: (i) the United Kingdom; or (ii) a country or sector deemed adequate pursuant to the Data Protection Law applicable in the UK;
"Customer Data"	means the Personal Data transmitted by the Customer to Cognism pursuant to the Agreement, as set out in Annex 1, Part 1 herein (Details of Data Processing – Controller-to-Processor processing of Customer Data);
"Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed by either Party pursuant to the Agreement, whilst such Protected Data is in the custody or control of the other Party;
"Data Protection Law"	means the law and regulation applicable to processing of Personal Data under the Agreement, including but not limited to European Law and US Law;
"European Law"	means the law and regulation of the European Union ("**EU**"), the European Economic Area ("**EEA**"), their member states, Switzerland, and the United Kingdom applicable to the processing of Personal Data under the Agreement (including, as applicable, (i) Regulation 2016/679 of the European Parliament and of the Council 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) ("**EU GDPR**"); (ii) the EU GDPR as retained into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Data Protection Act in force from 1 September 2023 and its corresponding ordinances ("**Swiss DPA**"); (iv) the EU e-Privacy Directive (Directive 2002/58/EC); and (v) any amending, updating or replacing legislation or regulation from time to time in force;
"EU SCCs"	means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to the EU GDPR;
"Protected Data"	means the Customer Data and the Profile Data transmitted, stored or otherwise processed pursuant to this Agreement;

"Profile Data"	means the Personal Data transmitted by Cognism or made available to the Customer pursuant to the Services, as set out in Annex 1, Part 2 herein (Details of Data Processing – Controller-to-Controller processing of Profile Data);
"Services"	means those services provided by Cognism under the Agreement as set out in the relevant Order Form;
"Supervisory Authority"	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;
"UK SCC Addendum"	means version B1.0 of the international data transfer addendum to the EU Commission Standard Contractual Clauses issued by the ICO pursuant to section 119A(1) of the Data Protection Act 2018, and any replacement or updated version thereof adopted in accordance with the Data Protection Laws or otherwise recognised or endorsed by the ICO
"US Law"	means the law and regulation of the United States applicable to the processing of Personal Data under the Agreement, including (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (Cal. Civ. Code § 1798.100 - 1798.199, 2022) and its implementing regulations ("**CCPA**"), (ii) the Virginia Consumer Data Protection Act, when effective, (iii) the Colorado Privacy Act and its implementing regulations, when effective, (iv) the Utah Consumer Privacy Act, when effective; and (v) Connecticut SB6, An Act Concerning Personal Data Privacy and Online Monitoring, when effective, (vi) the Texas Data Privacy and Security Act of 2023, when effective, (vii) the Tennessee Information Protection Act, when effective, (viii) the Oregon Consumer Privacy Act of 2023, when in force, (ix) the Montana Consumer Data Privacy Act of 2023, when in force, (x) the Indiana Consumer Data Protection Act of 2023, when in force, (xi) the Iowa Data Privacy Act of 2023, when in force, (xii) the Delaware Personal Data Privacy Act of 2023, when in force, (xiii) the applicable data protection laws made at federal or state level from time to time in force; and any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i) - (xiii) and any amending, updating or replacing legislation or regulation from time to time in force.

2.2. For the purposes of this DPA, "**controller**", "**processor**", "**data subject**", "**Personal Data**" and "**process**" shall have the meanings set out in the EU GDPR and "**process**" and "**processed**", will be construed accordingly, and will include both manual and automatic processing.

3. NATURE OF DATA PROCESSING

3.1. Scope and Application of the DPA. For the purpose of providing the Services under the Agreement, both Parties will receive and process Personal Data. This DPA applies to all (i) Customer Data; and (ii) Profile Data.

3.2. Respective Roles and Responsibilities. The Parties agree that (a) with regards to Customer Data, the Customer is the Controller and Cognism is the Processor, and (b) with regards to Profile Data, both Cognism and the Customer will process such data as independent controllers.

3.3. Nature and Details of Processing. The nature and details of Processing are set forth in Annex 1 to this DPA (Details of Data Processing), Part 1 of the Annex sets out the details of the processing activities in relation to Customer Data (Details of Data Processing – Controller-to-Processor), and Part 2 sets out the details of the processing activities in relation to Profile Data (Details of Data Processing – Controller-to-Controller).

3.4. Mutual Obligations. The Parties shall at all times comply with their respective obligations under Data Protection Laws and with their respective obligations under this DPA in connection with the processing of the Protected Data as part of the Services provided under the Agreement.

4. CUSTOMER PERSONAL DATA PROCESSING

4.1. Cognism Obligations. Insofar as Cognism processes Customer Data on behalf of the Customer, Cognism shall (a) unless required to do otherwise to ensure compliance with Data Protection Laws, only act upon and process Customer Data in accordance with the Customer's instructions as set out in Annex 1 to this DPA, or as otherwise provided by the Customer to Cognism in writing from time to time ("Processing Instructions"). If Cognism believes that any Processing Instruction received by it from the Customer is likely to infringe the Data Protection Laws, it shall promptly inform the Customer and be entitled to cease to provide the relevant Services until the parties have agreed appropriate amended instructions which are not infringing. The Subscription Fees payable to Cognism shall not be discounted or set-off as a result of any delay or non-performance of any obligation in accordance with this clause 4.1 (a); (b) ensure that the personnel who has access to Customer Data (i) receive adequate training in compliance with this DPA and Data Protection Laws; (ii) are under an obligation to maintain the security and confidentiality of any Customer Data which they have access to, and (iii) do not process Customer Data other than in accordance with the Processing Instructions, unless as otherwise required under applicable law; (c) taking into account the nature of the processing, take all appropriate technical and organisational measures, Cognism shall, at the Customer's cost, co-operate with and provide all necessary assistance to enable the Customer to comply with its obligations under Articles 32 to 36 (inclusive) of the EU GDPR in relation to the Customer Data or any other equivalent obligations under other applicable Data Protection Laws including in relation to respond to any requests from any data subject(s) and/or any Supervisory Authority; (d) notify the Customer without undue delay, and in any event within 48 hours, upon becoming aware of a Data Breach relating to Customer Data; (e) where processing Customer Data on behalf of the Customer within the scope of the CCPA, not retain, use, or disclose such personal data for any purposes other than the purposes set out in the Agreement and this DPA and as permitted under the CCPA, including under any "sale" exemption; and (f) cease processing of the Customer Data and, at the Customer's written request, either delete or return the Customer Data after the business purposes for which the Customer Data was processed have been fulfilled or terminated, whichever is earlier, unless continued processing is required under Applicable Data Protection Law.

4.2. Customer Obligations. The Customer represents and warrants that (a) the Customer Data which it supplies or discloses to Cognism under the Agreement has been obtained fairly and lawfully; (b) it has provided all necessary fair processing information to data subjects and obtained all necessary and appropriate consents from them to enable (i) the Customer to lawfully transfer the Customer Data to Cognism; and (ii) Cognism to process the Customer Data in accordance with this DPA and the Agreement; (c) the Processing Instructions will not breach, and will not cause Cognism to breach, applicable Data Protection Law; and (d) the Customer Data is accurate, up-to-date and not excessive or irrelevant in relation to the purposes for which Cognism will process the Customer Data.

4.3. Sub-Processors. Cognism is hereby authorised by the Customer to engage its Affiliates and third party service providers as listed in annex 1 herein ("Approved Sub-Processors") to process the Customer Data as sub-processors as required to enable Cognism to fulfil its obligations under the Agreement. In the event Cognism intends to add or replace any Approved Sub-Processor, Cognism shall inform the Customer in order to give the Customer the opportunity to object to such changes within thirty (30) days, provided such objection is based on reasonable grounds relating to data protection. Cognism shall (i) ensure that the new sub-processor is contractually bound to substantially similar obligations as to the obligations under this DPA with respect to the processing of the Customer Data; and (ii) remain fully liable to the Customer for the sub-processors' acts or omissions with regards to its processing of the Customer Data.

4.4. Audit. Cognism will conduct audits of its security controls applied to the processing of the Customer Data. Each audit will be performed according to the rules of the accreditation body for each applicable control standard or framework and will be performed by qualified, independent, third-party security auditors at Cognism's selection and expense. Each audit will result in the generation of an audit report, which Cognism may make available to the Customer in a redacted version, subject to non-disclosure and distribution limitations of Cognism and the auditor. To the extent the Customer's audit requirements under applicable Data Protection Laws cannot reasonably be satisfied through the audit reports or other information Cognism makes generally available to the Customer, Cognism will respond to the Customer's additional requests to provide information to the extent necessary to demonstrate Cognism's compliance with its obligations as data processor under Article 28 of the GDPR. In the event an onsite audit of Cognism's premises is required, the Customer shall provide a reasonable prior written advance and before the commencement of such audit, Cognism and the Customer will, acting in good faith, mutually agree upon the scope, timing, duration, control and evidence requirements. The Customer agrees that

the audit will be conducted without unreasonably interfering with Cognism's business activities, during regular business hours and subject to Cognism's security policies and confidentiality procedures. Where onsite audits of physical data centers are not permitted, the Customer will work with Cognism to reach a mutually agreeable resolution sufficient to provide information necessary for the Customer to fulfil its obligations under applicable Data Protection Laws.

5. PROFILE DATA PROCESSING

5.1. Independent Controller Obligations. With regards to the processing of Profile Data, either party shall (a) ensure that it is not subject to any prohibition or restriction which would prevent or restrict it from disclosing or transferring the Personal Data to the other party, as required under this DPA; (b) ensure that all fair processing notices have been given and are sufficient in scope and kept up-to-date in order to meet the Transparency Requirements (as defined under Data Protection Law) to enable each party, subject to such party's own compliance with the Data Protection Law, to process the Personal Data under this DPA in accordance with the Data Protection Law. Each party must and will independently ensure that (i) they have a lawful basis for their Processing of such Personal Data, and (ii) such use and Processing of the Personal Data is compliant with the Data Protection Law; (c) ensure that the Personal Data is adequate, relevant, limited to what is necessary in relation to the permitted purpose and, where necessary, up-to-date; and (d) ensure that the Profile Data is transferred between the parties by a secure means.

5.2. Processing Activities. The transfer of Profile Data by Cognism is based on the Customer's business-to-business sales, marketing, recruiting, or business development activities as specified in the Agreement (collectively, "B2B Activities"). The Customer will only process the Profile Data for its B2B Activities or as otherwise permitted under the Agreement.

5.3. Cognism Warranties. Cognism hereby warrants that (a) it has collected all Profile Data provided to Customer as part of the Services in compliance with the Data Protection Laws; (b) it will promptly honor any opt-out requests it receives from data subjects in the Services in accordance with the Data Protection Law; and (c) it will make available to Customer a list of data subjects who have requested that their Personal Data be removed from the Services.

5.4. Customer Warranties. The Customer hereby warrants (a) it will process the Profile Data in compliance with applicable Data Protection Laws; and (b) it will comply promptly with any opt-out requests received by Cognism by deleting securely and permanently such Profile Data from their systems.

5.5. Technical and Organisational Security Measures. Each party shall implement and maintain (in accordance with Data Protection Law) appropriate technical and organisational measures taking into account the state of the art, the implementation costs, and the nature, scope, circumstances and purpose of the processing, as well as the different probability of occurrence and the severity of the risk of the rights and freedoms of the persons concerned in order to ensure a level of protection appropriate to such risk. Such measures shall at all times: (a) be of at least the minimum standard required by Applicable Data Protection Laws; (b) in respect of Cognism, comply with the measures as set out in Annex 2 herein ("**TOMs**"); and (c) be of a standard no less than the standard compliant with good industry practices for the protection of Personal Data.

5.6. Reporting. The parties shall each comply with its obligation under Data Protection Law to report a Data Breach to the appropriate supervisory authority and (where applicable) data subjects.

5.7. Data Subject Rights. The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Law within the time limits imposed by the Data Protection Law.

6. INTERNATIONAL TRANSFERS OF PERSONAL DATA

6.1. Non-Adequate Jurisdictions. To the extent Protected Data is transferred to other countries that have not been recognized under the Applicable Data Protection Laws as an Adequate Jurisdiction ("Non-Adequate Jurisdiction"), the relevant Standard Contractual Clauses ("**SCCs**") contained in Annex 3 to this DPA will apply.

6.2. Standard Contractual Clauses. For the purposes of the SCCs, the following additional provisions shall apply (a) with regards to Profile Data, Cognism shall be regarded as the data exporter and Customer shall be regarded as the data importer, (b) with regards to Customer Personal Data, the Customer shall be regarded as the data exporter

and Cognism shall be regarded as the data importer; (c) the parties agree to observe the terms of the SCCs without substantive modification, except as listed in Annex 5 (Standard Contractual Clauses) herein; and (d) In the event of any conflict between the provisions of (i) the SCCs; and (ii) the remaining terms of this DPA, then the SCCs, or any replacement thereof, shall take precedence. The terms of this DPA shall not vary the SCCs in any way.

7. US STATE PRIVACY LAWS

7.1. Compliance. To the extent that either party processes any Protected Data relating to individuals who are "consumers" as that term is defined in the applicable US Law, the party shall comply with the applicable requirements under the applicable US Law, and shall provide the same level of privacy protection as required by the applicable US Law, including by implementing and maintaining reasonable security procedures and practices appropriate to the nature of the Protected Data to protect the Protected Data from unauthorized or illegal access, destruction, use, modification, or disclosure.

7.2. CCPA. To the extent that Cognism processes any Customer Data relating to individuals who are California residents, Cognism shall, to the extent required by the applicable US Law: (a) grant the Customer the right to take reasonable and appropriate steps to help ensure that Cognism uses the Customer Data in a manner consistent with Cognism's obligations under the applicable US Law; (b) grant the Customer the right, upon reasonable notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of the Customer Data; and (c) promptly notify the Customer if Cognism determines that it can no longer meet its obligations under the applicable US Law.

8. LIABILITY

8.1. Each Party's liability under this DPA shall be construed in a manner consistent with the limitations of liability set out in the Agreement.

9. GOVERNING LAW AND JURISDICTION

9.1. This DPA and any non-contractual obligations arising out of or in connection with it shall be governed by and interpreted in accordance with the laws of England and Wales.

9.2. Each party irrevocably submits to the exclusive jurisdiction of the courts of London, England over any claim or matter arising under, or in connection with, this DPA.

ANNEX 1 – DETAILS OF PROCESSING ACTIVITIES

PART 1 – Controller-to-Processor processing of Customer Data

A. PARTIES

Controller:

Name of Customer	[INSERT]
Address of Customer	[INSERT]
Contact person's name, role and contact details	[INSERT]

Processor:

Name	Cognism Limited
Address	c/o Worldwide Corporate Advisors 30 - 34 New Bridge Street London EC4V 6BJ United Kingdom
Contact details	Cognism Privacy Team: privacy@cognism.com

B. DATA PROCESSING AND TRANSFER OF PERSONAL DATA

Subject matter and duration of the Processing of Personal Data	Cognism's provision of technology services to Customer as set out in the relevant Order Form and for the duration of the Agreement
The nature and purpose of the Processing of Personal Data	Cognism will be processing Customer Data as listed herein for account set up and account management purposes as necessary for Cognism to provide the Services to Customer pursuant to the Agreement.
Categories of Personal Data	Customer personnel [*data validation / enrichment – Customer business clients and prospects*]
Legal basis for processing	Performance of contract / Legitimate interest
Type of Personal Data	Name, business email address
Sensitive Data	None
Approved Sub-Processors	As listed here
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous for the duration of the Agreement.

PART 2 – Controller-to-Controller processing of Profile Data

A. PARTIES

Data exporter:

Name	Cognism Limited
Address	c/o Worldwide Corporate Advisors 30 - 34 New Bridge Street London EC4V 6BJ United Kingdom
Contact details	Cognism Privacy Team: privacy@cognism.com
Role (Controller/Processor)	Controller

Data importer:

Name of Customer	[INSERT]
Address of Customer	[INSERT]
Contact person's name, role and contact details	[INSERT]
Role (Controller/Processor)	Controller

B. DATA PROCESSING AND TRANSFER OF PERSONAL DATA

Subject matter and duration of the Processing of Personal Data	Cognism's provision of technology services to Customer as set out in the relevant Order Form and for the duration of the Agreement
The nature and purpose of the Processing of Personal Data	As necessary to provide the Services to Customer in accordance with the Agreement and this DPA, including Customer's B2B Activities.
Categories of Personal Data	Business personnel
Legal basis for processing	Legitimate interest
Type of Personal Data	Profile of contact data, including: name, employer, job title, business email address, business telephone number and LinkedIn URL.
Sensitive Data	None
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)	Continuous for the duration of the Agreement.

ANNEX 2

TOMs

1. Access Controls

Access controls ensure that access to Cognism systems, applications, and data is granted on a need-to-know, least-privilege basis, authenticated strongly, and reviewed on a recurring basis. The following measures govern how identities are provisioned, authenticated, authorised, monitored, and de-provisioned across the environment.

Identity Lifecycle & Authorisation

- Access is provisioned through standardized request workflows with formal approval aligned to defined role requirements
- Access rights are reviewed periodically to ensure continued appropriateness and compliance
- Access is managed using a Role-Based Access Control (RBAC) model aligned to job responsibilities
- Access is granted following the principle of least privilege
- All provisioning and access changes are logged and monitored within the SIEM
- MFA and SSO are enforced to strengthen authentication and access control across all systems where applicable

Additional high-level measures

- Privileged access is restricted and time-bound where feasible, and subject to enhanced monitoring and review
- Administrative access requires strong authentication, encrypted channels, and zero-trust access controls for remote administration
- Periodic access certifications are performed at least semi-annually for in-scope systems; remediation actions are tracked to completion

2. Vulnerability Management

Cognism maintains a continuous vulnerability management programme that identifies, prioritises, and remediates weaknesses across infrastructure, application code, and third-party dependencies. The programme combines automated scanning, manual testing, independent penetration testing, and a public disclosure channel, with remediation governed by internal service level agreements aligned to business risk.

Detection & Testing

- There is continuous vulnerability scanning of the infrastructure and code packages
- Tests include both automated tools and manual testing techniques (QA)
- Independent penetration testing is performed at least annually with documented remediation plans and verification
- There is an ongoing vulnerability disclosure program

Prioritisation & Remediation

- Vulnerabilities are tracked in our ticketing system with severity-based remediation timelines, and remediation is verified through retesting and validation scans before closure
- Vulnerabilities are prioritised depending on the real business risk, considering the exploitability, severity, CVSS, and EPSS score
- Vulnerabilities are tracked and remediated as per our internal SLAs

3. Secure Development Standard

Cognism's secure development standard governs how software and infrastructure are designed, built, reviewed, tested, and released. It combines environment separation, a formal Software Development Lifecycle (SDLC), secure coding

practices, and automated security controls in CI/CD pipelines to reduce the likelihood of vulnerabilities being introduced into production.

- Separated environments for development, staging and production
- A formal SDLC defines requirements for design, build, test (including security testing), approval, and release, including emergency changes
- Secure coding standards, secrets scanning, IaC, SAST, and SCA run in CI/CD
- Changes to infrastructure and application components are documented, tested in non-production, peer-reviewed, and approved prior to release

4. Logging, Monitoring & Detection

Cognism operates a centralised, always-on monitoring capability that combines log aggregation, threat detection, endpoint protection, and human-led response. The programme is designed to provide early detection of malicious activity, support investigations, and maintain visibility across cloud, application, and endpoint layers.

- Centralised logging (SIEM) collects security and audit events from cloud, application, and endpoint sources; alerts are triaged and investigated
- A 24/7 Security Operations Center (SOC) provides continuous security monitoring, detection, and incident response capabilities
- Intrusion detection/threat detection services monitor malicious activity across cloud accounts, networks, and endpoints
- Infrastructure and application health are monitored with alerting on performance and availability thresholds
- Malware protection is deployed on relevant systems with MDR functionality
- Cloud Security Posture Management (CSPM) tooling continuously monitors cloud environments for configuration drift, misconfigurations, and policy violations

5. Supplier & Cloud Security

Third parties and cloud service providers are integral to Cognism's service delivery. Supplier and cloud security measures ensure that providers are appropriately vetted prior to onboarding, contractually bound to security obligations, operated against hardened configuration baselines, and offboarded through controlled exit procedures.

Onboarding & Ongoing Assurance

- Third-party and cloud providers are assessed prior to onboarding and reviewed at least annually for security and availability commitments
- Contractual requirements include security controls, incident notification, and service levels; NDAs are executed before information sharing

Cloud Configuration & Offboarding

- Cloud environments follow secure configuration baselines; network segmentation, WAF, and firewall rule reviews help prevent unauthorised access
- Exit procedures ensure secure data export and deletion at the end of a relationship

6. Incident Response & Business Continuity

Cognism maintains documented incident response and business continuity capabilities to detect, respond to, and recover from security events and service disruptions. These capabilities are exercised on a regular basis and include defined roles, escalation paths, customer communications, and recovery objectives for critical services.

Incident Response

- A documented incident response plan defines roles, escalation paths, triage, containment, eradication, recovery, and post-incident review

- Regular simulated phishing campaigns are conducted to test employee awareness and resilience against social engineering attacks, with results used to inform targeted remediation and training
- Incidents and security events are logged, tracked to resolution, and communicated to relevant stakeholders in line with defined procedures
- Customer-facing channels exist for reporting service incidents or concerns

Business Continuity & Disaster Recovery

- Business Continuity and Disaster Recovery plans set RTO/RPO targets, roles, and communications; plans are exercised at least annually

7. Availability & Resilience

Availability and resilience measures ensure that Cognism's critical services remain operational under expected demand, recover quickly from disruption, and protect against data loss. Capacity is monitored continuously, backups are performed on a recurring basis to logically separate locations, and databases are replicated across geographic or logical fault domains.

- Capacity is monitored and scaled to meet demand; resilience patterns are used for critical services
- Production data is backed up at least daily to a logically separate location; restoration procedures are tested
- Databases are replicated to secondary regions or availability zones with alerting on replication failures
- DDoS protection and content delivery is enforced through a CDN and DDoS mitigation service, protecting the availability of customer-facing services against volumetric and application-layer attacks

8. Cryptography

Cognism uses cryptographic controls to protect personal data both in transit and at rest, supported by industry-standard key management practices. Encryption configurations are aligned with recognised best practice and enforced across databases, storage, and backups.

- Encryption in transit (TLS) with a minimum of TLS 1.2
- Encryption at rest (AES-256) is enforced for databases, data storage, and backups
- Key management follows industry best practices
- Globally used keys are AWS-managed keys

9. Physical & Environmental Security

Cognism's production infrastructure is operated within a leading cloud service provider, inheriting their physical and environmental controls under the shared responsibility model. Corporate offices implement controls proportionate to risk, and data-bearing assets are securely handled throughout their lifecycle.

- Production infrastructure is hosted within AWS, following the shared responsibility model
- Infrastructure is primarily deployed in eu-west-1 region (Ireland)
- Corporate offices use controlled entry, video surveillance, and secure areas where appropriate
- Employee laptops and mobile devices are enrolled in a Mobile Device Management (MDM) solution, enabling central policy enforcement and configuration management
- Asset disposal ensures data-bearing devices are securely wiped/destroyed prior to reuse or disposal

10. HR & People Security

People are a critical layer of Cognism's control environment. HR and people security measures address pre-employment screening, confidentiality obligations, disciplinary processes, and ongoing security and privacy awareness training for all personnel.

- Pre-employment screening is performed in accordance with local laws and role risk for both full-time employees and contractors

- Employees acknowledge confidentiality and acceptable use obligations
- Violations are subject to a disciplinary process
- Security and privacy awareness training is delivered upon hire and at least annually

11. Governance, Risk & Compliance

Cognism's governance, risk, and compliance programme provides the overarching framework within which all technical and organisational measures are designed, operated, and assured. The programme is governed by a documented policy framework, informed by regular risk assessments, and validated through internal and external reviews.

- An information security policy framework is documented, reviewed at least annually, and communicated to staff
- Risk assessments are performed at least annually, including consideration of fraud, regulatory, and technology changes
- Control self-assessments, internal audits, and management reviews evaluate ISMS and control effectiveness; corrective actions are tracked
- Cyber insurance is maintained to mitigate financial impact from security incidents and business disruptions

ANNEX 3

Standard Contractual Clauses ("SCCs")

I. Transfer Clauses Generally

With respect to transfers of Personal Data across national borders to other countries that have not been recognized under the Applicable Data Protection Laws as an Adequate Jurisdiction, the parties hereby agree to be bound by, where applicable:

(1) For transfers of Personal Data from an EEA Data Exporter to a Non-Adequate Jurisdiction, the Controller-to-Controller EU SCCs are deemed incorporated into this DPA in their entirety and without alteration, except as noted below. To the extent that the Data Importer is subject to the extra-territorial scope of Article 3(2) of the EU GDPR with respect to the specific processing, the obligations imposed on the Data Importer by the EU GDPR shall prevail over its obligations under the SCCs, where the latter are less strict. For reference, the official EU SCCs are available here;

(2) For transfers of Personal Data from a UK Data Exporter to a non-Adequate Jurisdiction, the SCCs (as referred to above in section (i)) and the UK SCC Addendum is applicable here;

(3) For transfers of Personal Data from any other applicable jurisdiction with SCCs, the relevant the Controller-to-Controller SCCs are deemed incorporated in their entirety and without alteration as required and relevant under such jurisdiction's applicable law.

II. EU SCCs

When both parties are acting as Controllers, and when the EEA Data Exporter transfers Personal Data to a non-Adequate Jurisdiction, Module 1 of the EU SCCs applies. With respect to Module 1 of the EU SCCs, the parties hereby further agree that:

(1) Clause 7 of the SCCs - Docking Clause applies;

(2) Clause 9 of the SCCs is intentionally omitted;

(3) the following provision under Clause 13(a) of Module 1 of the EU SCCs applies:

The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(4) the following provision under Clause 17 of Module 1 of the EU SCCs applies:

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The parties agree that this shall be the laws of the Republic of Ireland.

(5) the following provision under Clause 18(b) of Module 1 of EU the SCCs applies:

The parties agree that those shall be the courts of the Republic of Ireland.

(6) with respect to Annex I of the EU SCCs, the details of the data exporter and data importer are set forth in clause 6.2 of this DPA.

(7) with respect to Annex I of the EU SCCs the description of the transfer are set forth in Annex 1 of this DPA.

(8) with respect to Annex II of the EU SCCs the description of the technical and organisational security measures are set forth in Annex 2 of this DPA.

(9) with respect to Annex III of the EU SCCs the details of the sub-processors are set forth here.

III. Adjustments to the EU SCCs for Personal Data Transfers from Switzerland

A. To the extent that the Data Exporter is established in Switzerland and transfers Personal Data related only to Swiss data subjects to a Non-Adequate Jurisdiction, the Swiss DPA applies to the transfers of Personal Data and, therefore, the following adjustments to the EU SCCs shall apply to ensure an adequate level of protection for the transfers of Personal Data outside Switzerland in accordance with the Swiss DPA:

(1) Annex I.C under Clause 13 of the EU SCCs:

With regard to the Swiss entity as a data exporter, the competent supervisory authority is the Federal Data Protection and Information Commissioner ("FDPIC");

(2) Clause 17 of the EU SCCs:

The law governing the Standard Contractual Clauses is Swiss law;

(3) The use of the term 'EU Member State' in the EU SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EU SCCs;

(4) References to the EU GDPR in the EU SCCs are to be understood as references to the Swiss DPA.

B. To the extent that the Data Exporter is established in Switzerland and transfers Personal Data related (also) to EEA data subjects to a non-Adequate Jurisdiction, or if the transfers of Personal Data are otherwise subject to the extraterritoriality provisions of the EU GDPR (Article 3), the Swiss DPA and the EU GDPR apply in parallel to the transfers of Personal Data. In this case, the parties agree that the EU GDPR standard will apply to the transfers of Personal Data because the EU GDPR provides adequate protection and data subjects are consequently not disadvantaged as a result of the transfers. The following adjustments to the SCCs shall apply:

(1) Annex I.C under Clause 13 of the EU SCCs:

With regard to the Swiss entity as a data exporter, the competent supervisory authorities are the FDPIC, insofar as the transfers of Personal Data are governed by the Swiss DPA, and the EEA competent supervisory authority as indicated in Annex I.C of the EU SCCs, insofar as the transfers of Personal Data are governed by the EU GDPR;

(2) the use of the term 'EU Member State' in the EU SCCs must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 of the EU SCCs;

(3) with respect to Annex I of the EU SCCs, the details of the data exporter and data importer are set forth in clause 6.2 of this DPA.

(4) with respect to Annex I of the EU SCCs the description of the transfer are set forth in Annex 1 of the DPA.

(5) with respect to Annex II of the EU SCCs the description of the technical and organisational security measures are set forth in Annex 2 of this DPA.

(6) with respect to Annex III of the EU SCCs the details of the sub-processors are set forth here.

IV. UK SCC Addendum

With respect to the UK SCC Addendum, the parties agree that:

(1) with respect to Table 1 of the UK SCC Addendum, the details of the data exporter and data importer are set forth in clause 6.2.1 of the DPA;

(2) with respect to Table 2 of the UK SCC Addendum, the version of the SCCs in force at the date of execution of this DPA applies;

(3) with respect to Table 3 of the UK SCC Addendum, (a) the description of the parties is set forth in clause 6.2 of this DPA, (b) the details of the processing are set forth in Annex 1 of this DPA, and (c) the description of the technical and organisational security measures are set forth in Annex 2 of this DPA;

(4) with respect to Table 4 of the UK SCC Addendum, no parties may end the UK SCC Addendum as set out in Section 19 of the UK SCC Addendum.