DATA PROCESSING ADDENDUM

Annex B to the Master Services Agreement

Sofia Connect EAD · v1.0 · Effective Date: as set out in the Service Order

---

Parties

This Data Processing Addendum ("DPA") forms an integral part of the Master Services Agreement ("MSA") entered into between Sofia Connect EAD and the Customer (the "Agreement"). Capitalized terms used and not defined herein have the meaning given to them in the MSA.

Provider / Processor: Sofia Connect EAD, a joint-stock company organized under the laws of the Republic of Bulgaria, having its registered office at 192A Cherni Vrah Blvd, 1407 Sofia, Bulgaria, UIC: 204636154, VAT: BG204636154 ("Sofia Connect" or "Processor").

Customer / Controller: the legal entity identified in the relevant Service Order or Service Order Form executed under the MSA ("Customer" or "Controller").

The Parties have entered into the MSA pursuant to which Sofia Connect provides electronic communications, network and connectivity services to the Customer (the "Services"). To the extent Sofia Connect Processes Personal Data on behalf of the Customer in the course of providing the Services, the Parties agree to comply with the terms of this DPA.

1. Definitions

"Applicable Data Protection Law" means (i) Regulation (EU) 2016/679 (the "GDPR"); (ii) the Bulgarian Personal Data Protection Act (Закон за защита на личните данни, ЗЗЛД) and any implementing regulations; (iii) Directive 2002/58/EC (ePrivacy) as transposed into Bulgarian law; and (iv) any other applicable laws, regulations and binding guidance issued by supervisory authorities in respect of the Processing of Personal Data.

"Personal Data" means any information relating to an identified or identifiable natural person Processed by Sofia Connect on behalf of the Customer in the course of providing the Services, as further described in Schedule 1 (Processing Particulars).

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

"Sub-processor" means any third-party processor engaged by Sofia Connect to Process Personal Data on behalf of the Customer.

"Standard Contractual Clauses ("SCCs")" means the standard contractual clauses approved by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, as may be amended, superseded or replaced from time to time.

"Controller", "Processor", "Data Subject", "Processing" and "Supervisory Authority" have the meanings given to them in the GDPR.

2. Subject Matter, Roles and Scope

2.1 The Customer is the Controller and Sofia Connect is the Processor in respect of the Personal Data Processed by Sofia Connect on behalf of the Customer in the course of providing the Services. Sofia Connect shall not Process Personal Data for any purpose other than the performance of the Services or as documented in the Customer's instructions.

2.2 The duration, nature and purpose of the Processing, the categories of Personal Data Processed and the categories of Data Subjects are set out in Schedule 1 (Processing Particulars).

2.3 Where Sofia Connect Processes Personal Data as a Controller in its own right — for example, in respect of (i) network traffic and signalling data necessary for the operation, security and integrity of the network under Article 6(1)(b) and (f) GDPR, (ii) statutory data retention obligations under the Bulgarian Electronic Communications Act (Закон за електронните съобщения), or (iii) billing and contract administration with the Customer — such Processing is governed by Sofia Connect's Privacy Policy at https://sofia-connect.net/legal/privacy/ and not by this DPA.

3. Obligations of the Processor

3.1 Sofia Connect shall Process Personal Data only on documented instructions from the Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Bulgarian law; in such a case, Sofia Connect shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.2 The MSA, this DPA, and the relevant Service Order constitute the Customer's complete and final documented instructions to Sofia Connect for the Processing of Personal Data. Any additional or alternate instructions must be agreed in writing by both Parties; if a Customer instruction would in Sofia Connect's reasonable opinion infringe Applicable Data Protection Law, Sofia Connect shall inform the Customer without undue delay.

3.3 Sofia Connect shall ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and have received appropriate training on their data protection responsibilities.

3.4 Sofia Connect shall implement and maintain the technical and organisational measures ("TOMs") set out in Schedule 2 (Technical and Organisational Measures), and shall, 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, ensure a level of security appropriate to the risk pursuant to Article 32 GDPR.

3.5 Taking into account the nature of the Processing, Sofia Connect shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights under Chapter III of the GDPR. Sofia Connect shall promptly notify the Customer of any Data Subject request it receives directly and shall not respond to such requests except on documented Customer instructions.

3.6 Sofia Connect shall assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (security, breach notification, impact assessments and prior consultation), taking into account the nature of Processing and the information available to Sofia Connect.

3.7 At the choice of the Customer, Sofia Connect shall delete or return all Personal Data to the Customer after the end of the provision of the Services, and delete existing copies unless Union or Bulgarian law requires storage.

Statutory retention obligations under the Bulgarian Electronic Communications Act and the Bulgarian Accountancy Act survive termination of the Services.

3.8 Sofia Connect shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, as set out in Section 8 (Audits) below.

4. Obligations of the Controller

4.1 The Customer warrants that: (i) it has a valid legal basis under Article 6 GDPR (and, where applicable, Article 9 GDPR) for the Processing carried out by Sofia Connect; (ii) it has provided all required notices and obtained any necessary consents from Data Subjects; and (iii) its instructions to Sofia Connect comply with Applicable Data Protection Law.

4.2 The Customer shall not provide to Sofia Connect any special categories of Personal Data under Article 9 GDPR or criminal-conviction data under Article 10 GDPR, except as expressly agreed in writing and documented in Schedule 1.

5. Sub-processors

5.1 The Customer hereby grants Sofia Connect a general written authorisation to engage Sub-processors for the performance of the Services, subject to the conditions set out in this Section 5.

5.2 The current list of authorised Sub-processors is set out in Schedule 3 (Sub-processors). Sofia Connect shall maintain an up-to-date version of this list and shall publish it at https://sofia-connect.net/legal/dpa/sub-processors/.

5.3 Sofia Connect shall inform the Customer of any intended addition or replacement of Sub-processors at least thirty (30) days before the change takes effect. The Customer may object to such change on reasonable data protection grounds within fifteen (15) days of receiving the notice. If the Parties cannot resolve the objection in good faith, the Customer may terminate the affected Services without penalty as its sole and exclusive remedy.

5.4 Sofia Connect shall impose on each Sub-processor, by way of a written contract, data protection obligations no less protective than those set out in this DPA. Sofia Connect shall remain fully liable to the Customer for the performance of each Sub-processor's obligations.

6. International Data Transfers

6.1 Sofia Connect shall not transfer Personal Data outside the European Economic Area ("EEA") except in accordance with Chapter V of the GDPR.

6.2 Where Sofia Connect (or any Sub-processor) transfers Personal Data to a country that has not been the subject of an adequacy decision under Article 45 GDPR, the Parties shall rely on the Standard Contractual Clauses, which are hereby incorporated by reference and shall apply as follows:

- Module Two (Controller to Processor) shall apply where the Customer is established in the EEA and Sofia Connect transfers Personal Data to a Sub-processor outside the EEA.
- Module Three (Processor to Sub-processor) shall apply where Sofia Connect, acting as Processor, onward-transfers Personal Data to a Sub-processor outside the EEA.

- Clause 7 (docking clause) is not used. Clause 9(a) — Option 2 (general written authorisation) is used, with the time period set out in Section 5.3 above. Clause 11(a) — the optional independent dispute-resolution body language is not used. Clause 17 — these SCCs shall be governed by the laws of the Republic of Bulgaria. Clause 18(b) — disputes shall be resolved before the courts of Sofia, Bulgaria. Annexes I, II and III to the SCCs are deemed populated by Schedules 1, 2 and 3 to this DPA respectively.

6.3 The Parties shall carry out a transfer impact assessment where required and shall implement supplementary measures (such as strong encryption in transit and at rest, key management under EEA jurisdiction, and pseudonymisation) as appropriate to ensure an essentially equivalent level of protection.

7. Personal Data Breach Notification

7.1 Sofia Connect shall notify the Customer without undue delay, and in any event within seventy-two (72) hours after becoming aware of a Personal Data Breach affecting the Customer's Personal Data.

7.2 The notification shall, to the extent possible at the time, contain: (i) a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the name and contact details of Sofia Connect's data protection contact; (iii) a description of the likely consequences of the Personal Data Breach; and (iv) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.3 Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. Sofia Connect shall reasonably cooperate with the Customer in any subsequent investigation, remediation, notification to supervisory authorities and communications to Data Subjects.

7.4 Notifications shall be sent to the Customer's data protection contact email address recorded in the relevant Service Order and, in parallel, to any e-mail address marked as "security" or "privacy" notified to Sofia Connect in writing. Sofia Connect's notifications shall be issued from privacy@sofia-connect.net.

8. Audits and Inspections

8.1 Sofia Connect shall make available to the Customer, upon written request and no more than once per calendar year (unless required following a Personal Data Breach or by a Supervisory Authority), information reasonably necessary to demonstrate compliance with this DPA, including the most recent third-party certifications and audit reports available to Sofia Connect (such as ISO/IEC 27001 statements of applicability and SOC 2 Type II reports of Sub-processors, where available).

8.2 Where such information is reasonably insufficient to demonstrate compliance, the Customer may, at its own cost and on at least thirty (30) days' prior written notice, audit Sofia Connect's compliance with this DPA. Audits shall be conducted during regular business hours, shall not unreasonably interfere with Sofia Connect's operations, and shall be subject to confidentiality undertakings.

8.3 Sofia Connect may require the Customer (and any auditor mandated by the Customer) to sign a non-disclosure agreement and shall not be required to give access to: (i) data of Sofia Connect's other customers; (ii) Sofia Connect's internal accounting or financial information; (iii) any trade secret of Sofia Connect; or (iv) information which, in Sofia Connect's reasonable opinion, would compromise the security of Sofia Connect's systems or premises or cause Sofia Connect to breach its obligations under Applicable Data Protection Law or under any other agreement.

9. Liability and Indemnity

9.1 The aggregate liability of either Party under or in connection with this DPA shall be subject to the limitation of liability provisions set out in the MSA, except where mandatory law (including Article 82 GDPR) provides otherwise.

9.2 Each Party shall indemnify the other for any administrative fines imposed by a Supervisory Authority, or compensation awarded to Data Subjects under Article 82 GDPR, to the extent such fines or compensation are attributable to that Party's breach of this DPA or of Applicable Data Protection Law.

10. Term, Termination and Survival

10.1 This DPA takes effect on the Effective Date of the MSA and remains in force for as long as Sofia Connect Processes Personal Data on behalf of the Customer.

10.2 Sections relating to confidentiality, liability, audit (in respect of completed Processing), international transfers (in respect of any Personal Data still held), breach notification (for Personal Data Breaches occurring before termination) and return/deletion of Personal Data shall survive termination of the MSA.

11. Governing Law and Jurisdiction

11.1 This DPA, including the SCCs incorporated by reference, shall be governed by and construed in accordance with the laws of the Republic of Bulgaria, without regard to its conflict-of-laws rules.

11.2 The courts of Sofia, Bulgaria shall have exclusive jurisdiction over any dispute arising out of or in connection with this DPA, subject to the rights of Data Subjects under Article 79 GDPR.

11.3 The competent supervisory authority for Sofia Connect is the Commission for Personal Data Protection of the Republic of Bulgaria (Комисия за защита на личните данни), located at 2 Prof. Tsvetan Lazarov Blvd, 1592 Sofia, Bulgaria, https://www.cpdp.bg.

12. Order of Precedence

12.1 In the event of any conflict or inconsistency between this DPA, the MSA and the SCCs, the order of precedence shall be: (i) the SCCs (where they apply); (ii) this DPA; (iii) the MSA; and (iv) any Service Order.

13. Data Protection Contact

13.1 Sofia Connect's data protection contact is: privacy@sofia-connect.net. The Customer's data protection contact is the address recorded as such in the Service Order, or, in its absence, the address used for billing notices.

Schedule 1 — Processing Particulars (SCC Annex I)

A. List of Parties

Data exporter (Controller): the Customer, as identified in the Service Order. Data importer (Processor): Sofia Connect EAD, address as set out in the Parties section above. Contact: privacy@sofia-connect.net.

B. Description of Transfer

Item	Description
Categories of Data Subjects	Customer's employees, contractors, end-users, customers and other contacts whose Personal Data is transmitted across the network as part of the Services. Sofia Connect does not have visibility into the content of Customer traffic except as required for security and integrity of the network.
Categories of Personal Data	(a) Service administration: name, business email, business phone, role of authorised Customer contacts; (b) Network operations: source/destination IP addresses, port numbers, BGP routing data, traffic volumes, timestamps, and similar metadata; (c) Support tickets: any Personal Data the Customer chooses to include in support requests; (d) Optional CPE telemetry where the Customer opts in.
Special categories of data	None expected. Should the Customer require Processing of special categories, this must be expressly agreed and documented in writing under Article 9 GDPR.
Frequency of transfer	Continuous for the duration of the Services.
Nature of Processing	Transmission, routing, switching, peering, traffic management, monitoring, troubleshooting, security operations, capacity planning, and storage of operational logs.
Purpose of Processing	Provision of the electronic communications and connectivity Services described in the MSA and the applicable Service Order(s).
Period of retention	Operational logs: 12 months by default, then aggregated or deleted, except where longer retention is required by the Bulgarian Electronic Communications Act, the Accountancy Act, or a lawful order. Support tickets: 24 months after closure. Administrative contact data: for the duration of the contract plus the statutory limitation period (5 years).
Transfers to Sub-processors	See Schedule 3. Subject matter and duration as set out in the relevant Sub-processor contracts.

C. Competent Supervisory Authority

The Commission for Personal Data Protection of the Republic of Bulgaria (Комисия за защита на личните данни), as supervisory authority of the Processor's main establishment in the EEA.

Schedule 2 — Technical and Organisational Measures (SCC Annex II)

Sofia Connect implements and maintains the following technical and organisational measures to ensure a level of security appropriate to the risk pursuant to Article 32 GDPR. These measures are reviewed at least annually and updated to reflect changes in the state of the art.

1. Information Security Governance

- Documented Information Security Management System aligned with ISO/IEC 27001:2022 principles; security policies reviewed at least annually.
- Named security and data protection contact (privacy@sofia-connect.net); incident response runbook and 24/7 NOC capability.
- Security awareness and data protection training for all personnel on hire and at least annually thereafter.

2. Access Control

- Role-based access control on the principle of least privilege; access to production systems requires multi-factor authentication.
- Quarterly access reviews for production systems and customer-facing portals; immediate revocation upon role change or departure.
- Privileged operations are logged and reviewed; session recording for jump-host access.

3. Network and Infrastructure Security

- Segmented management plane; out-of-band management network; restricted SSH/NETCONF/gNMI access with key-based authentication only.
- BGP route filtering with RPKI Origin Validation, peer authentication with MD5/TCP-AO, and uRPF where applicable.
- DDoS detection and mitigation on the IP transit edge; perimeter ACLs; traffic anomaly monitoring.
- Edge devices and OOB equipment patched on a documented cadence with critical CVE response within 72 hours where operationally feasible.

4. Cryptography

- TLS 1.2 or higher with strong cipher suites for all customer-facing portals and APIs.
- Configuration data, secrets and tokens stored encrypted at rest using AES-256 (or equivalent) with managed key rotation.
- Email transport secured with opportunistic TLS and DANE where available; DKIM, SPF and DMARC enforced on sofia-connect.net.

5. Physical Security

- Equipment hosted in Tier-III or equivalent carrier-neutral data centres (e.g., Telepoint, Equinix, NTT, Interxion) with 24/7 manned security, biometric or card-based access control, CCTV, and environmental controls.
- Customer cross-connect access controlled via written authorisation and ticketing.

6. Operations Security

- Centralised log collection with tamper-evident storage; retention as set out in Schedule 1.
- Configuration management with peer review for production changes; back-out plans for risky changes.
- Vulnerability scanning of internet-facing assets on at least a monthly cadence; remediation prioritised by CVSS.
- Backups of configuration data with restore tests at least twice per year.

7. Business Continuity and Resilience

- Diverse fibre routes and dual power feeds at all core PoPs; geographically diverse routing for inter-city links.
- Documented disaster recovery procedures; restoration targets aligned with SLA commitments.
- 24/7 NOC with documented escalation matrix; on-call rotation for security incidents.

8. Personnel

- Background checks for personnel with access to customer data, to the extent permitted by applicable law.
- Binding confidentiality and data protection clauses in employment and contractor agreements.

9. Sub-processor Management

- Pre-engagement security and data protection due diligence for new Sub-processors.
- Written data protection terms with each Sub-processor no less protective than this DPA.
- Annual review of critical Sub-processors based on certifications, incidents and continued necessity.

10. Data Subject Rights and Breach Response

- Documented procedures to assist the Customer with Data Subject requests and Personal Data Breach notification within the timeframes set out in Section 7.
- Incident severity matrix mapped to NOC response targets; security incidents escalated to the data protection contact within one business hour of identification.

Schedule 3 — Authorised Sub-processors (SCC Annex III)

The following Sub-processors are authorised by the Customer as of the Effective Date of this DPA. The current version of this list is maintained at https://sofia-connect.net/legal/dpa/sub-processors/. Notifications of changes are governed by Section 5 of this DPA.

Sub-processor	Service	Location of Processing	Categories of Data
DE-CIX Management GmbH	Internet exchange peering at Frankfurt, Madrid and other DE-CIX locations	Germany / EEA	BGP signalling, peer identification, traffic statistics
Equinix (Germany / Netherlands / UK / Bulgaria)	Data centre colocation and cross-connect provision	EEA / United Kingdom	Physical access logs and cross-connect administration
Telepoint EAD	Data centre colocation in Sofia	Bulgaria / EEA	Physical access logs and cross-connect administration
Hetzner Online GmbH	Compute and hosting for selected back-office systems	Germany / Finland (EEA)	Operational metadata; no customer Personal Data processed for the Services unless explicitly agreed
Cloudflare, Inc.	DNS, WAF and CDN for sofia-connect.net public assets	Global anycast (with EEA data localisation where available)	Public website visitor IP, request logs (no customer Service Personal Data)
Vercel Inc.	Hosting of the sofia-connect.net marketing site and customer portal preview	United States / EEA (region: fra1 by default)	Public website visitor IP, request logs (no customer Service Personal Data)
Google LLC (Google Analytics 4, Google Workspace)	Website analytics and corporate email/collaboration	EEA / United States (under EU-US Data Privacy Framework)	Website analytics events; business contact data
Microsoft Corporation (Microsoft 365)	Corporate email, collaboration and storage for Sofia Connect personnel	EEA (with US fallback under DPF)	Business contact data; email content where Customer correspondence is stored
Resend, Inc.	Transactional email delivery for customer notifications	United States (under DPF) / EEA	Recipient email address, message metadata
Supabase, Inc.	Managed Postgres for selected portal back-end services	EEA region (Frankfurt)	Portal account metadata; no Customer traffic data

Notes: (i) Cross-connect providers (Equinix, Telepoint and similar) act as Processors only in respect of physical access administration data and as Controllers of their own facility data. (ii) Public website analytics and transactional email Sub-processors do not Process Personal Data transmitted across the Customer's connectivity Service; they are listed here in the interest of transparency in respect of the Sofia Connect business relationship.

Превод на български език (информативен)

Настоящият превод на български език е предоставен с информативна цел. В случай на несъответствие между английския оригинал и българския превод, английският текст има предимство.

СПОРАЗУМЕНИЕ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Анекс Б към Рамковия договор за услуги

София Кънект ЕАД · в. 1.0 · В сила: съгласно посоченото в Заявката за услуга

Страни по договора

Настоящото Споразумение за обработване на лични данни („Споразумение“, „DPA“) представлява неразделна част от Рамковия договор за услуги, сключен между София Кънект ЕАД и Клиента („Договорът“). Термините, използвани с главна буква и неопределени тук, имат значението, дадено им в Договора.

Доставчик / Обработващ лични данни: София Кънект ЕАД, акционерно дружество, регистрирано по законите на Република България, със седалище: гр. София 1407, бул. Черни връх 192А, ЕИК: 204636154, ДДС № BG204636154 („София Кънект“ или „Обработващ“).

Клиент / Администратор на лични данни: юридическото лице, посочено в относимата Заявка за услуга, сключена по силата на Рамковия договор („Клиент“ или „Администратор“).

1. Предмет и роли

1.1 Клиентът е Администратор, а София Кънект е Обработващ по отношение на личните данни, обработвани от София Кънект при предоставянето на услугите. София Кънект обработва лични данни единствено по документирани указания на Клиента, освен ако правото на ЕС или българското право не изисква друго.

1.2 Когато София Кънект обработва лични данни като самостоятелен Администратор (напр. трафични данни, необходими за управлението и сигурността на мрежата по чл. 6, пар. 1, б. „б“ и „е“ GDPR; задължения за съхранение по Закона за електронните съобщения; фактуриране), такова обработване не се урежда от настоящото Споразумение, а от Политиката за поверителност на София Кънект, достъпна на https://sofia-connect.net/legal/privacy/.

2. Задължения на Обработващия

- Обработване единствено по документирани указания на Клиента; уведомяване при потенциално нарушаващо указание.
- Поверителност на персонала; задължителни клаузи за поверителност и обучения по защита на данните.
- Поддържане на технически и организационни мерки (вж. Приложение 2) съгласно чл. 32 GDPR.
- Съдействие на Клиента при упражняване на правата на субектите на данни и при оценки на въздействието.
- Връщане или изтриване на личните данни при прекратяване на услугите, освен ако законът изисква запазване.
- Предоставяне на информация за съответствие и допускане на одити в рамките на Раздел 8.

3. Подобработващи и международни предавания

3.1 Клиентът предоставя обща писмена оторизация за ангажиране на подобработващи съгласно списъка в Приложение 3. София Кънект уведомява Клиента най-малко 30 дни преди добавяне или замяна на подобработващ. Клиентът има право да възрази в срок от 15 дни на разумни основания, свързани със защита на личните данни. При неуспех на добросъвестно разрешаване, Клиентът може да прекрати засегнатата услуга без неустойка.

3.2 При предаване на лични данни извън ЕИЗ към държави без решение за адекватно ниво на защита, страните прилагат Стандартните договорни клаузи на Европейската комисия (Решение за изпълнение (ЕС) 2021/914), Модул 2 и/или Модул 3, които се считат за включени по препратка с настоящото Споразумение.

4. Уведомление при нарушение

София Кънект уведомява Клиента без неоправдано забавяне и във всеки случай в срок до 72 (седемдесет и два) часа след узнаване за нарушение на сигурността на личните данни, засягащо личните данни на Клиента. Уведомлението съдържа описанието по чл. 33, пар. 3 GDPR, доколкото е възможно към момента на уведомяване, и се изпраща от privacy@sofia-connect.net.

5. Приложимо право и юрисдикция

Настоящото Споразумение се урежда от законите на Република България. Споровете се разглеждат от съдилищата в гр. София. Компетентният надзорен орган е Комисията за защита на личните данни на Република България (КЗЛД), бул. „Проф. Цветан Лазаров“ № 2, 1592 София, https://www.cpdp.bg.

6. Контакт

Контакт по защита на личните данни в София Кънект: privacy@sofia-connect.net.

За пълните условия, технически и организационни мерки и списъка с подобработващи, моля направете справка с английския оригинал в първата част на настоящия документ.

Signatures / Подписи

This DPA is executed in two counterparts, one for each Party. Electronic signature under the eIDAS Regulation (EU) No 910/2014 is acceptable.

For and on behalf of Sofia Connect EAD

Name: Yuliy Nushev

Title: Chief Executive Officer

Signature: _____

Date: _____

Email: nushev@sofia-connect.net

For and on behalf of the Customer

Name: _____

Title: _____

Signature: _____

Date: _____

Email: _____