

FRAMEWORK AGREEMENT ON MANAGED BUG BOUNTY PROGRAM SERVICES

This Framework Agreement is entered into between

SPRIND GmbH,

Lagerhofstraße 4, 04103 Leipzig, represented by the Managing Directors Mrs. Berit Dannenberg and Mr. Rafael Laguna de la Vera,

– hereinafter referred to as ‘Client’ –

and

the bidder selected in the procurement procedure

acting upon award of the contract,

address and authorised representative as submitted in the tender

– hereinafter referred to as ‘Service Provider’ –

– Client and Service Provider together hereinafter referred to as the ‘Parties’–

Contents

1.	Preamble.....	3
2.	Contractual documents and Order of Precedence	3
3.	Subject Matter and Scope of Services.....	3
4.	Asset Scope and Restrictions.....	4
5.	Obligations of Service Provider	4
6.	Obligations of Client	5
7.	No contractual relationship between Client and Security Researchers	5
8.	Term.....	5
9.	Service Provider Fee, Reward and Payment Process	6
10.	Rights in Work Results	7
11.	Confidentiality.....	7
12.	Data Protection and Controllorship	7
13.	Security and Compliance Requirements.....	8
14.	Liability and Indemnification	8
15.	Insurance	8
16.	Final provisions and Governing Law.....	8
	Annex A – List of Definitions.....	10
	Annex B – Service Description and Requirements	12
	Annex C – Service Level Agreement (SLA).....	21
	Annex D – List of In-Scope Systems and Assets.....	23
	Annex E – Vulnerability Disclosure Policy (VDP).....	24
	Annex F – Pricing and Payment	27
	Annex G – Template Solution concept	28
	Annex H – Template CVs	30
	Annex I – Data Processing Agreement and Standard Contractual Clauses	35
	Appendix 1 to Annex I – Details of the Processing	42
	Appendix 2 to Annex I – Technical and Organizational Measures including Technical and Organisational Measures to ensure the security of the data	43

1. Preamble

On 29 May 2026 Client launched the call for tenders under the reference EIN-1464 for the provision of managed bug bounty program Services.

This Framework Agreement is concluded as a result of a public procurement procedure conducted by Client in accordance with applicable public procurement law. Service Provider was selected at the conclusion of the evaluation process, on the basis of its tender submitted on [date] in response to the invitation to tender.

This Framework Agreement's purpose is to define the terms and conditions under which Service Provider shall provide managed bug bounty program Services.

The Framework Agreement aims to support Client in enhancing the security of its digital infrastructure through authorised, coordinated, and legally compliant security testing activities.

2. Contractual documents and Order of Precedence

- 2.1. This Framework Agreement consists of the Framework Agreement and the following annexes, which form an integral part of the Framework Agreement
 - Annex A – List of Definitions
 - Annex B – Service Description and Requirements
 - Annex C – Service Level Agreement (SLA)
 - Annex D – List of In-Scope Systems and Assets
 - Annex E – Vulnerability Disclosure Policy (VDP)
 - Annex F – Pricing and Payment
 - Annex G – Template Solution Concept
 - Annex H – Template CVs
 - Annex I – Data Processing Agreement (DPA) and Standard Contractual Clauses.
- 2.2. In the event of any inconsistencies or contradictions between the contractual documents, the following order of precedence shall apply:
 1. The Bidder Questionnaire including the answers of the Client as awarding authority
 2. The Framework Agreement
 3. The Annexes in the order listed above (**Annex A to G**)
 4. Any other documents referenced during the procurement procedure.
- 2.3. In the event of any contradiction, inconsistency or deviation between the provisions of the Framework Agreement and its Annexes and any solution concepts or other tender documents submitted by the Bidder, the Framework Agreement and its Annexes shall take precedence.

3. Subject Matter and Scope of Services

- 3.1. Service Provider shall set up and manage a managed Bug Bounty Program (BBP) on behalf of Client. The goal is to harden Client's systems against sophisticated threats by incentivising independent Security Researchers to identify and report vulnerabilities via a BBP.
- 3.2. Service Provider's Services shall include, but are not limited to planning, launching, and administering bug bounty campaigns or continuous testing programs, recruiting

and managing participation of Security Researchers, validating Security Researchers' submitted vulnerability reports, providing remediation recommendations for Validated Findings. Further details are set out in **Annex B** (Service Description and Requirements) and **Annex C** (Service Level Agreement).

- 3.3. Services shall be provided as required on the basis of individual call-of-orders placed by Client. Each individual order must be made in writing; an order placed by email is sufficient for this purpose.
- 3.4. The members of Client's Management are authorised to place individual orders. They may authorise other employees of Client in writing to call of Services under this Framework Agreement. Authorisation by email is sufficient to satisfy the written form requirement.
- 3.5. The Framework Agreement is subject to a maximum call-off volume of 2,400,000 € net over the maximum total term (including all extension options).

4. Asset Scope and Restrictions

- 4.1. In-Scope Assets
The systems, applications, and Services authorised for testing under this Framework Agreement ('In-Scope Assets') are initially listed in **Annex D** (In-Scope Assets and Restrictions).
- 4.2. Client may, at its sole discretion, update In-Scope Assets during the term of the Framework Agreement. Such updates may include the addition, removal, or replacement of assets. These updates shall be made by written instruction (e.g., via email).
- 4.3. Service Provider shall ensure that the current list of In-Scope Assets is accurately published and maintained on the designated bug bounty platform used for the Program.
- 4.4. In the event of any discrepancy between **Annex D** (In-Scope Assets and Restrictions) and the asset list published on the platform, the version published on the platform shall prevail, provided that such publication has been authorised in writing by Client.
- 4.5. Out-of-Scope Assets
Systems, applications, and Services that are not explicitly listed as In-Scope Assets in **Annex D** (In-Scope Assets and Restrictions) shall be considered out of scope for testing under this Framework Agreement.

5. Obligations of Service Provider

- 5.1. Service Provider shall deliver the Services in accordance with this Framework Agreement and the Service Description (**Annex B**).
- 5.2. Service Provider shall implement appropriate contractual, organisational and technical measures within its bug bounty platform and processes that are reasonably designed to promote and enforce compliance with the Vulnerability Disclosure Policy (VDP) as set out in **Annex E** (Vulnerability Disclosure Policy (VDP)).
- 5.3. Service Provider shall publish the current version of the VDP on the bug bounty platform in a clear and accessible manner. Service Provider shall ensure that all potential Security Researchers have the opportunity to become aware of the VDP and explicitly agree to its terms prior to submitting any Vulnerability Reports. Service Provider shall coordinate with Client on any updates to the VDP and ensure timely implementation of approved changes.

- 5.4. Service Provider shall cooperate with Client in the investigation, clarification, and assessment of reported vulnerabilities, and shall encourage the participating Security Researchers to cooperate accordingly.
- 5.5. Service Provider shall comply with all applicable laws and regulations, including but not limited to cybersecurity and data protection laws, and shall encourage the participating Security Researchers to also comply with these requirements. Only submissions in accordance with the VDP shall be accepted and awarded by Service Provider.
- 5.6. Service Provider shall provide the Services using the platform, tools, and methodologies described in its submitted tender in response to the invitation to tender under reference EIN-1464, including as set out in its solution concept submitted as part of that tender. Any material deviation from the tendered platform or solution concept requires prior written approval by Client.
- 5.7. Service Provider shall designate that the key personnel identified in the CVs submitted as part of its tender as primary point of contact in respect of the Services. Any replacement of such primary point of contact requires prior written approval by Client, which shall not be unreasonably withheld. Service Provider shall ensure that any replacement contact personnel have qualifications and experience at least equivalent to those of the personnel originally proposed.

6. Obligations of Client

- 6.1. Client shall define the overall scope and objectives of the Bug Bounty Program. It shall approve the list of In-Scope Assets and any updates thereto, as well as the Vulnerability Disclosure Policy (VDP) and any amendments.
- 6.2. Client shall approve the initial bounty reward table proposed by Service Provider and may modify or adjust this proposal.
- 6.3. Client shall oversee and coordinate remediation activities and retains final decision-making authority on the eligibility of bounty payments and the classification of vulnerability severity.
- 6.4. Client shall take decisions within a reasonable time on issues escalated by Service Provider, including confirmation or adjustment of severity classifications, bounty eligibility and amounts, and proposed changes to scope or program policies, to avoid undue delays in program operations and researcher communication.

7. No contractual relationship between Client and Security Researchers

No direct contractual relationship shall exist between Client and individual Security Researchers participating in the Bug Bounty Program. Service Provider shall act as the sole contractual counterparty for all researchers and shall pass on all relevant obligations and restrictions to them.

8. Term

- 8.1. This Framework Agreement shall enter into force upon signature by both Parties and shall become effective on the date of the contract award by Client.
- 8.2. The Framework Agreement shall remain in force for a fixed term of 12 months from the effective date. Ordinary termination during the fixed term is excluded. The right of either Party to terminate the Framework Agreement for good cause (Clause 8.3) remains unaffected. The Framework Agreement shall automatically extend for a further period of twelve (12) months unless Client notifies Service Provider in writing not later than (thirty) 30 days before the end of the then current term that no such extension shall

take effect. Automatic extension pursuant to this Clause may occur on no more than two occasions.

- 8.3. Each Party shall have the right to terminate this Framework Agreement for good cause with immediate effect. Good cause shall include, but shall not be limited to, incorrect information provided by Service Provider in the award procedure, material breach of contractual obligations by the other Party, repeated failure to meet agreed service levels, insolvency or imminent insolvency of the other Party, legal or regulatory changes that make the continuation of the Framework Agreement unlawful or impracticable.
- 8.4. In the event that Service Provider is permanently unable to perform its obligations under this Framework Agreement – including, but not limited to, as a result of termination for good cause pursuant to Clause 8.3, the opening of insolvency proceedings over the assets of Service Provider, or any other circumstances that permanently preclude continued performance – Client reserves the right to offer the remaining Services to the other bidders or bidding consortia that participated in the underlying award procedure under reference EIN-1464, in the order of their ranking in that procedure up to and including the fifth-ranked bidder, on the basis of the tenders submitted by those bidders in that procedure.

9. Service Provider Fee, Reward and Payment Process

- 9.1. Service Provider shall receive an annual fee for the provision of Services under this Framework Agreement, comprising two components: a General Platform Fee and a Triage Service Fee (together the “Total Fee”). The applicable Total Fee is determined by the pricing tier (Tier A through Tier I) that corresponds to the Maximum Annual Bounty To Spend authorised by Client for the relevant term, as set out in **Annex F** (Pricing and Payment). This Total Fee covers all obligations and deliverables set out in the Framework Agreement and its annexes. For the avoidance of doubt, the Total Fee constitutes the sole and entire remuneration payable by Client to Service Provider in connection with the Services, and no additional fees, charges, costs, expenses, or disbursements of any kind shall be payable by Client unless separately agreed in writing by both parties in advance.
- 9.2. The applicable pricing tier shall be determined at the beginning of each term (pursuant to Clause 8.2) based on the Maximum Annual Bounty To Spend agreed in writing by the Parties for that term independent from the amount transferred into the Trust Account. If, during the term of this Framework Agreement, the cumulative bounty disbursements reach the Maximum Annual Bounty To Spend of the then-applicable tier, the fees applicable to the higher tier as defined in **Annex F** (Pricing and Payment) shall automatically apply from the date on which the higher tier is reached; however, for the remainder of the relevant term, Client shall only pay the difference between the fees already applicable to the previously applicable pricing tier and the fees of the higher pricing tier. The Parties shall document the date of the tier change in writing. Tier downgrades shall take effect only from the beginning of the next contract term or billing period, unless the Parties agree otherwise in writing.
- 9.3. All bounty rewards to Security Researchers will be disbursed via a designated Trust Account managed by Service Provider. Service Provider shall be responsible for:
 - Organising and administering bounty payments in an orderly manner, including the applicable payment process, as further specified in **Annex F** (Pricing and Payment).

- Ensuring that bounty payments are made only after validation and approval of reported vulnerabilities by Client.
 - Ensuring timely and secure payment of bounties to eligible researchers.
 - Maintaining a transparent and auditable record of all bounty transactions including an up-to-date overview of the available and committed bounty budget at all times.
 - Complying with applicable financial and tax regulations in Germany and the EU.
- 9.4. Service Provider shall ensure that bounty disbursements do not at any time exceed the funds standing to the credit of Client's bounty account, such that the balance of such account shall not at any time become negative. Any increase to the Maximum Annual Bounty To Spend other than by way of an automatic tier upgrade pursuant to Clause 9.2 requires prior written approval by Client.

10. Rights in Work Results

- 10.1. Service Provider shall ensure that all reports, remediation documentation, and other work results delivered by Service Provider under this Framework Agreement – including any such work product created by participating Security Researchers – may be used by Client without restriction for the contractually agreed purposes and for the fulfilment of Client's statutory and regulatory obligations (including reporting duties towards supervisory authorities).
- 10.2. Service Provider shall not demand, require, or enforce any exclusive rights, exclusive licences, or ownership in any other form over Security Researchers' submissions made under Client's Bug Bounty Program, to the extent such rights would restrict Client's ability to use the submissions as set out in this Framework Agreement. Service Provider may obtain and rely on a non-exclusive licence from Security Researchers only to the extent necessary to operate the bug bounty platform, perform triage and validation, manage communication with researchers, and administer bounty payments in accordance with this Framework Agreement.
- 10.3. The rights granted to Client under Clause 10.1 shall include the right to publish work results, including any patches or fixes contributed by Security Researchers, under an applicable open-source licence.

11. Confidentiality

- 11.1. The Parties undertake to treat as strictly confidential all information obtained in the context of this Framework Agreement, including vulnerability findings and any information that becomes known to participating Security Researchers. Such information shall be used solely for the purpose of fulfilling contractual obligations under this Framework Agreement.
- 11.2. Service Provider shall ensure that all participating Security Researchers are bound by confidentiality obligations.
- 11.3. This confidentiality obligation shall remain in effect beyond the termination or expiration of this Framework Agreement.

12. Data Protection and Controllorship

- 12.1. Service Provider shall comply with all applicable laws, including the EU General Data Protection Regulation (EU GDPR).
- 12.2. The Parties acknowledge that it is not envisaged that any Personal Data will be processed in connection with this Framework Agreement. To the extent that Personal Data

is processed, each Party act as an independent controller within the meaning of Article 4(7) GDPR.

- 12.3. Notwithstanding the foregoing, where any processing of Personal Data requires the Service Provider to act as a processor on behalf of the Client within the meaning of Article 4(8) GDPR, the Parties shall, prior to any such processing, enter into a data processing agreement (DPA). Where required under applicable law, the Parties shall further execute the applicable Standard Contractual Clauses (SCCs). The form of DPA, including the SCCs, is attached to this Framework Agreement as **Annex I** (Data Processing Agreement (DPA) and Standard Contractual Clauses).

13. Security and Compliance Requirements

- 13.1. Service Provider shall implement and maintain an appropriate security management system, including information security management and security incident management, in accordance with recognized industry standards.
- 13.2. Service Provider shall ensure compliance with the ISO/IEC 27001, the SOC2 Type 2 or any other equivalent standard, as applicable, and shall provide evidence of such compliance upon request by Client.
- 13.3. Service Provider shall take all necessary measures to ensure compliance with the requirements of the NIS 2 Directive (Directive (EU) 2022/2555) and any applicable national implementing legislation, insofar as the Services provided under this Framework Agreement fall within its scope.
- 13.4. Client shall have the right to conduct security assessments and audits to verify Service Provider's compliance with the security requirements set out in this Framework Agreement. Service Provider shall cooperate fully with such assessments and provide access to relevant documentation, systems, and personnel, subject to reasonable notice.

14. Liability and Indemnification

- 14.1. Service Provider shall be liable to Client for damages in accordance with the applicable statutory provisions. No further contractual limitations or extensions of liability shall apply unless expressly agreed otherwise in this Framework Agreement.
- 14.2. The Service Provider shall be liable towards the Client for any loss or damage caused by third parties engaged by the Service Provider in the performance of this Framework Agreement to the same extent as if the Service Provider had caused such loss or damage itself.

15. Insurance

Service Provider shall maintain, for the duration of this Framework Agreement, professional liability insurance with a minimum coverage amount of EUR 1,000,000 per claim covering personal injury, property damage, and financial loss. Proof of valid insurance coverage shall be provided to Client upon request at any time.

16. Final provisions and Governing Law

- 16.1. Amendments and additions to this Framework Agreement, including any changes to annexes, must be made in writing. This also applies to any waiver of the written form requirement.
- 16.2. This Framework Agreement shall be governed by and construed in accordance with the laws of the Federal Republic of Germany.

- 16.3. The place of jurisdiction is Leipzig. If Service Provider is a merchant within the meaning of the German Commercial Code (HGB), a legal entity under public law, or a special fund under public law, the registered office of Client shall be the exclusive place of jurisdiction for all disputes arising out of or in connection with this Framework Agreement. Client is nevertheless entitled to bring an action at Service Provider's place of business as well. Any exclusive statutory place of jurisdiction shall take precedence.
- 16.4. If any provision of this Framework Agreement is or becomes invalid or unenforceable, the remaining provisions shall remain unaffected. The Parties shall replace the invalid or unenforceable provision with a valid provision that comes as close as possible to the economic intent of the original.

Annex A – List of Definitions

1. **Framework Agreement** – this contract, including its main body and all annexes, which sets forth the binding terms and conditions agreed between Client and Service Provider.
2. **Services** – the managed bug bounty program Services to be performed by the Service Provider as described in this Framework Agreement (particularly **Annex B**).
3. **Management** – the members of the project management of the EUDI Wallet project of the Client. This includes the Client's chief project officer of the EUDI Wallet and any deputies or delegates notified in writing to the Service Provider.
4. **EUDI Wallet / National German EUDI Wallet** – mobile application and backend infrastructure designed to securely store and share digital documents (e.g., ID cards, driver's licenses, university credentials) with legal certainty.
5. **Bug Bounty Program** – (Managed) Bug Bounty Program or BBP means the coordinated vulnerability discovery program operated under this Framework Agreement, whereby Security Researchers analyse In-Scope Assets to identify and report vulnerabilities and receive bounties as financial compensation based on the report validity and vulnerability severity.
6. **Third Party Systems** – any systems, applications, platforms, Services, or infrastructure components that are not designated as In-Scope Assets and that are not owned or operated on behalf of Client, including but not limited to systems of relying parties and issuers.
7. **Platform or Bug Bounty Platform** – the online system provided and operated by the Service Provider for running the Bug Bounty Program (including submission, communication, and reward disbursement features).
8. **In-Scope Assets** – the systems, applications, and Services expressly authorised for testing under this Framework Agreement, as initially listed in **Annex D** (and as updated by the Client in writing from time to time).
9. **Out-of-Scope Assets** – any systems, applications, or Services that are not designated as In-Scope Assets (including, for example, third-party systems not listed in **Annex D**), which are not authorised for testing under this Program.
10. **Vulnerability Report** – a submission by a Security Researcher describing a suspected security vulnerability including details required for the Service Provider to verify and evaluate the issue.
11. **Validated Findings** – vulnerability reports that have been confirmed by the Service Provider as genuine security vulnerabilities within the In-Scope Assets (i.e., the reported issue was successfully reproduced and determined to be valid).
12. **Security Researchers** – individuals (natural persons) who participate in the bug bounty program by attempting to identify and report security vulnerabilities in the In-Scope Assets.

- 13. Trust Account** – a dedicated account managed by the Service Provider on behalf of the Client, used exclusively for holding and disbursing bounty reward funds to Security Researchers under the bug bounty program.
- 14. Vulnerability Disclosure Policy (VDP)** – the document (**Annex E**) outlining the rules, guidelines, and procedures for responsibly disclosing vulnerabilities under the Bug Bounty Program.
- 15. Rules of Engagement** – set of program-specific rules defining permitted and prohibited actions for Security Researchers (usually outlined within the VDP or program terms).
- 16. Safe Harbour** – the assurance given by the Client that Security Researchers will not face legal action for their authorised, good-faith testing activities under the Program, provided they adhere to all Program rules.
- 17. Personal Data** – any information relating to an identified or identifiable natural person within the meaning of Article 4(1) of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR).
- 18. Bounty** – a monetary reward paid to a Security Researcher by Service Provider out of the Trust Account upon Client's validation and approval of a vulnerability report submitted in accordance with the Program Rules, the amount of which is determined by Client based on the severity and impact of the reported vulnerability.
- 19. Maximum Annual Bounty To Spend** – the maximum aggregate amount of Bounties authorised by Client to be disbursed to Security Researchers during a given term, as agreed in writing by the Parties and corresponding to the applicable pricing tier set out in **Annex F** (Pricing and Payment).

Annex B – Service Description and Requirements

This Service Description defines the technical and operational requirements for the provision of a managed Bug Bounty Program (BBP) for the German EU Digital Identity (EUDI) Wallet ecosystem.

The EUDI Wallet is a mobile application and backend infrastructure designed to securely store and share digital documents (e.g., ID cards, driver's licenses, university credentials) with legal certainty.

The requirements set out in this **Annex B** are divided into mandatory requirements and desirable, non-mandatory requirements. Mandatory requirements constitute binding minimum service requirements under this Framework Agreement and must be fulfilled by the Service Provider. In addition to the mandatory requirements, this **Annex B** sets out desirable, non-mandatory requirements that are preferred from Client's perspective and will positively influence the qualitative evaluation of the tender.

1. Obligations of Service Provider

1.1. Program Setup and Management

Mandatory Requirements

- 1.1.1 Service Provider shall establish and operate a managed Bug Bounty Program (BBP) for the EUDI Wallet ecosystem as a public program from the outset (no private pre-phase).
- 1.1.2 This includes providing platform Services, triage, researcher management, reporting, and bounty fund administration.
- 1.1.3 Service Provider is responsible for meeting the objectives of the BBP. The objectives of the BBP are:
 - To identify and triage security vulnerabilities in in-scope systems;
 - To establish a legally secure Safe Harbor Framework for white-hat researchers;
 - To ensure governance, auditability, and policy lifecycle control;
 - To outsource researcher relations and international payout management;
 - To promote global reach and attract qualified researchers through competitive bounty incentives.

Desirable, Non-Mandatory Requirements

None.

1.2. Scope of Services & Performance

Service Provider shall deliver all Services required for the full lifecycle of the bug bounty program. This encompasses:

Mandatory Requirements

- 1.2.1. Submission Handling

Providing an intake mechanism for Vulnerability Reports (with filtering of spam including low-quality AI-generated submissions without merit, duplicates and out-of-scope submissions).

1.2.2. Triage & Validation

Validating and assessing incoming vulnerability submissions (including reproducing issues in a controlled environment and assigning a severity and impact rating, subject to Client's final approval).

1.2.3. Tracking & Integration

Tracking progress for confirmed vulnerabilities and integrating with Client's internal ticketing system (e.g. Jira) for seamless hand-off and status synchronization.

1.2.4. Bounty Management

Administering bounty reward payments via the Trust Account including maintaining an up-to-date balance and transaction history accessible to Client.

1.2.5. Program Reporting

Providing ongoing reports and dashboards on program activity, including real-time KPI dashboards and periodic summary reports as requested.

Desirable, Non-Mandatory Requirements

None.

1.3. Platform Requirements

Service Provider shall provide and maintain a bug bounty platform with the following capabilities and standards:

Mandatory Requirements

- 1.3.1. The platform must support all stages from submission intake to closure, with a complete audit trail and state transparency.
- 1.3.2. Implement role-based access control (with admin, program admin, member, auditor roles, or equivalent roles) and require multi-factor authentication (MFA) for all user accounts with access to non-public data.
- 1.3.3. Provide integrated communication channels for interactions (e.g. between Client and triage team, and with researchers), including a secure agreed upon real-time channel for urgent discussions.
- 1.3.4. Publish and enforce the agreed Rules of Engagement (RoE) and Safe Harbor policy on the platform, ensuring researchers must accept these terms to participate. The platform must provide the flexibility to explicitly exclude specific services, products, or testing categories from the scope of authorised testing.
- 1.3.5. Enable bi-directional integration with Client's internal systems (e.g. Jira), including automated ticket creation for validated bugs, status updates synchronization, and configurable workflows to align with internal processes.
- 1.3.6. Protect all data transmitted across the platform (data in transit) and all data stored on the platform (data at rest) using industry-standard encryption mechanisms. Key management practices must also meet industry standards to ensure the confidentiality and integrity of all program data.

- 1.3.7. Maintain version control for program policies (VDP, RoE, Safe Harbor, payout rules) and retain historical versions for audit.
- 1.3.8. Implement a data retention policy that defines how long program data (reports, communications, logs, etc.) are kept and ensure secure deletion or anonymization after those periods and at the end of the contract term.
- 1.3.9. The platform must support easy, low-friction submission of vulnerability reports. No identification shall be required for initial submission, if not otherwise agreed upfront.

Desirable, Non-Mandatory Requirements

- 1.3.10. The platform shall support integration with external enterprise Identity Providers (e.g. via SAML 2.0 and/or OpenID Connect) to enable Single Sign-On and enforcement of Client's internal MFA policies.
- 1.3.11. Provide an option to embed an anonymous submission form on Client's website or security page, allowing external researchers to submit findings directly into the program.

1.4. Communication between Service Provider and Client

Mandatory Requirements

- 1.4.1. Communication between Service Provider and Client shall take place via the following channels:
 - Platform-integrated messaging features
 - Secure real-time communication channel for urgent or high-priority issues
 - Regular coordination calls (e.g., weekly or bi-weekly) to review program status, open items, and strategic developments
- 1.4.2. Service Provider shall designate a primary point of contact (e.g. Customer Success Manager). In addition, Service Provider shall designate a Triage team lead to answer questions from the Client. Any changes to these roles must be communicated to the Client without undue delay.

Desirable, Non-Mandatory Requirements

None.

1.5. Ticketing System Integration

Mandatory Requirements

Service Provider shall provide bi-directional integration with Client's internal Jira ticketing system.

The integration shall support:

- Automatic creation of tickets for validated vulnerabilities
- Synchronization of status updates and comments
- Export of triage reports and related file attachments
- Configurable workflows, field mappings, and notification rules

Communication on individual tickets shall primarily take place between Service Provider's triage team and the designated technical contacts of Client. Roles and access rights shall be defined during the onboarding phase.

Desirable, Non-Mandatory Requirements

The integration shall support export of triage summaries (as defined in 1.7.6).

1.6. Compliance and Governance

Mandatory Requirements

1.6.1. In order to grant access to Service Provider's platform, Service Provider shall ensure that the personnel and any other individuals engaged in performing or participating in the Services are appropriately educated, trained, fully qualified and available for the Services they are to perform, and possess specific regulatory, environmental or safety-related expertise where this is relevant to the relevant work areas. Such personnel shall be adequately familiar with Client's environment and requirements in order to perform the Services. Service Provider shall further ensure that all personnel and subcontractors with logical or physical access to production environments or other non-public program data are subject to appropriate and documented personnel security screening, in accordance with applicable law and industry practice, before such access is granted. Whenever Service Provider indicates that a member of its personnel has a specific level of experience, expertise or qualification, Service Provider warrants that such person in fact possesses such experience and expertise. Upon request of Client, Service Provider shall provide evidence of such experience, expertise, qualification, training and personnel screening. Except as otherwise expressly set forth in this Framework Agreement and its Annexes, Service Provider shall provide adequate continuous education and training to such personnel throughout the term of the Framework Agreement.

Furthermore, Service Provider shall:

- 1.6.2. Adhere to all applicable laws, including data protection (GDPR) and cybersecurity regulations. Ensure the program aligns with the EU NIS 2 Directive requirements to the extent applicable (e.g. incident handling and notification procedures).
- 1.6.3. Maintain an appropriate information security management system. At minimum, Service Provider must be certified under ISO/IEC 27001 or compliant with equivalent standards (such as SOC2 Type 2) and provide evidence of such certification/compliance upon request.
- 1.6.4. Provide Client with an up-to-date overview of all countries in which Client's data under this Framework Agreement is stored and processed, and of any locations outside the EU/EEA from which Service Provider's or its sub-processors' personnel may have logical access to such data (e.g. follow-the-sun support regions). This overview shall distinguish between primary hosting locations and remote support/access locations.
- 1.6.5. Maintain and provide to Client an up-to-date list of all sub-processors that are involved in providing the core Services under this Framework Agreement, including used cloud providers. The list shall indicate the role of each sub-processor (e.g. hosting, email delivery, payment processing) and the main processing location. Ensure and provide evidence that sub-processors are subject to the same level of security.
- 1.6.6. Warrant that all sub-processors engaged in the processing of personal data under this Framework Agreement are bound by data processing agreements that impose data protection obligations equivalent to those set out herein, comply with the requirements of the GDPR, and, where required, have entered into Standard Contractual

Clauses or any successor mechanism recognized as providing adequate safeguards under applicable data protection law.

- 1.6.7. Have documented incident response and disaster recovery plans for the platform. Have clearly defined Recovery Time Objective (RTO) / Recovery Point Objective (RPO) time-lines for service restoration in case of a platform breach or outage. In the event of a confirmed security incident or data breach affecting Client's data or the availability or integrity of the Services, Service Provider shall notify Client without undue delay and in any case within 24 hours after confirmation. The notification shall contain the information reasonably available at that time, including at least a description of the incident, its likely impact, and the initial mitigation measures taken or planned. Service Provider shall provide further updates as more information becomes available.
- 1.6.8. Operate a documented vulnerability and patch management process for its own platform and underlying components, including third-party and open-source libraries. For critical vulnerabilities (e.g. CVSS base score ≥ 9.0) affecting the Services, Service Provider shall implement appropriate mitigations or deploy fixes within a defined internal SLA and inform Client of any vulnerabilities that materially impact the security of the Services.
- 1.6.9. Acknowledge Client's right to conduct security audits and assessments. Upon reasonable notice, Service Provider shall cooperate fully with audits (by providing access to relevant systems, personnel, documents) and furnish current audit reports or certifications (e.g. ISO audit results) on request. Service Provider must also subject its platform and processes to regular independent security assessments (penetration tests, vulnerability scans) and, on request, share summary results or remediation evidence with Client.
- 1.6.10. Implement a comprehensive Non-Disclosure Agreement covering both Service Provider personnel and program participants. Ensure that no vulnerability details or sensitive information are disclosed publicly by any party without Client's prior written consent (see also Part II on Security Researcher obligations). This includes requiring Security Researchers to agree to confidentiality rules as part of the program terms.

Desirable, Non-Mandatory Requirements

- 1.6.11. All Personal Data under this Framework Agreement shall be stored, processed and effectively controlled in accordance with GDPR within the European Union or a non-EU country that has a fully adequate level of data protection without limitations (in line with https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

1.7. Managed Triage Services

Service Provider shall provide expert triage and validation for all incoming reports:

Mandatory Requirements

- 1.7.1. Maintain a dedicated triage team with proven expertise in relevant domains: i.a. web application security, authorization and identity protocols, wallet ecosystems, mobile app security, cryptography. Triage staff must be capable of handling complex vulnerabilities and must be fluent in vulnerability assessment methodologies.

- 1.7.2. Review and filter submissions - automatically and manually - to eliminate spam, out-of-scope reports, duplicates, or low-quality (e.g. AI-generated without merit) reports.
- 1.7.3. For each valid submission, independently reproduce the reported issue in a controlled environment. If full reproduction is not feasible, perform alternative verification (such as code analysis) and document the rationale.
- 1.7.4. Apply and communicate transparent, consistent criteria for handling duplicate reports, closing reports, resolving severity disputes, and communicating with researchers.
- 1.7.5. Assign an initial severity (e.g. using CVSS v3.1 or comparable metrics) and an initial impact rating to each validated vulnerability. Client reserves the right to adjust severity and impact based on internal risk considerations, but Service Provider's assessment should follow industry standards and be well-justified.
- 1.7.6. For each validated finding, prepare a comprehensive report summary to Client including clear reproduction steps, the necessary conditions to trigger the issue, impacted components, screenshots or proof-of-concept code as appropriate, and an initial recommendation for remediation. Each summary must be available via the platform.
- 1.7.7. Adhere to the agreed Service Level targets for triage. This includes meeting or exceeding the First Response Time and Triage Completion Time goals defined in **Annex C** (Service Level Agreement (SLA)) for various severity levels and maintaining the required platform availability. Service Provider shall monitor SLA performance and include SLA metrics in the regular program reports/ dashboards.
- 1.7.8. Any submission initially assessed by Service Provider as Exceptional or Critical, or otherwise indicating a plausible risk of active exploitation, substantial data exposure, systemic compromise, or material threat to service continuity, shall be escalated to Client immediately through the agreed emergency communication channel.

Desirable, Non-Mandatory Requirements

None.

1.8. Security Researcher & Bounty Management

Service Provider is responsible for effectively managing researcher participation and the bounty pool:

Mandatory Requirements

- 1.8.1. Leverage its platform's community and outreach mechanisms to attract skilled, reputable Security Researchers to the program. Particular effort should be made to reach researchers with expertise in the program's technology domains (as listed in 1.7.1). Service Provider should also moderate researcher participation, ensuring only those who agree to program rules and meet any eligibility criteria can submit.
- 1.8.2. Administer bounty payments to eligible Security Researchers worldwide, including researchers located outside the European Union and the European Economic Area, provided that such payments are permitted under applicable law and successfully pass all required identity verification, tax compliance, anti-money-laundering, and sanctions-screening checks. Service Provider shall promptly inform Client of any country-specific payout restrictions that may materially limit researcher participation in the Program.

- 1.8.3. Perform identity verification of researchers as needed for payout (Know-Your-Customer), handle any tax documentation or withholding if applicable, and conduct sanctions list screening. Under no circumstances shall bounties be paid to researchers who are on EU or international sanctions lists. Service Provider must have controls to prevent this.
- 1.8.4. Manage the bounty reward fund under the agreed Trust Account. Maintain a real-time ledger of the bounty budget, including the initial funding, amounts awarded, and remaining balance. This ledger must be accessible to Client upon request (e.g. through the platform or regular reports). Service Provider shall ensure bounty payments are issued promptly after a Vulnerability Report has been validated, but only after explicitly approved by Client, and only to the extent sufficient bounty funds are available under the Trust Account.
- 1.8.5. If the program ends or at any point upon Client's request, facilitate the return of any unallocated bounty funds from the Trust Account back to Client's account without undue delay and without additional fees.
- 1.8.6. Propose and maintain a bounty reward table (payment amounts for different vulnerability severities/categories) that is competitive and aligned with current market standards. This bounty table should be reviewed periodically (e.g. quarterly) with Client and adjusted by mutual agreement to remain attractive to researchers and effective in disincentivizing black-market sales of vulnerabilities.

Desirable, Non-Mandatory Requirements

- 1.8.7. Collect and relay feedback from researchers and from Client to continuously improve the program. This includes feedback on scope (e.g. suggestions to clarify or expand in-scope assets), on policy (e.g. clarity of rules), and on triage quality. Service Provider should use this feedback to recommend program adjustments and address any researcher concerns promptly (subject to Client's approval for any changes).

1.9. Analytics, Transparency & Reporting

Service Provider shall offer full transparency into the program's operations and outcomes:

Mandatory Requirements

- 1.9.1. Provide Client with access to an online dashboard showing real-time program metrics (e.g. number of reports, status breakdown, mean time to triage, etc.).
- 1.9.2. Key Performance Indicators: Track and report key KPIs, at a minimum: total submissions, validated vulnerabilities, distribution by severity, average triage times, bounty amounts paid, and any SLA compliance figures. Client may request additional metrics or publish certain metrics externally at its discretion (Service Provider should support such publication, e.g. by ensuring data can be exported without researcher PII).
- 1.9.3. Upon request, provide a structured data export of all program information for audit or archival purposes. This includes a full list of submissions and their details, the history of program policy versions/changes, all communications with researchers (in anonymized form if required), and complete records of the bounty pool transactions.
- 1.9.4. In addition to the live dashboard, deliver periodic summary reports (e.g. monthly or quarterly), highlighting trends, notable discoveries, and actions taken. These reports

should be suitable for internal security governance and, if needed, for reporting to supervisory authorities or management boards.

Desirable, Non-Mandatory Requirements

- 1.9.5. Key Performance Indicators: Track and report additional KPIs such as budget forecast, vulnerability types, recurring vulnerability patterns.
- 1.9.6. Provide API access for KPI retrieval and data export.

1.10. Onboarding Phase

Mandatory Requirements

Before the public launch, Service Provider shall support a time-limited onboarding phase. During the onboarding, Service Provider must set up the program environment, assist in finalising the VDP and Rules of Engagement, and validate the workflow end-to-end. Service Provider shall ensure a smooth transition from the onboarding phase to the full public program, carrying over all valid findings and learned improvements.

Desirable, Non-Mandatory Requirements

None.

1.11. Communication & Points of Contact:

Service Provider shall maintain effective communication channels and designated personnel for this engagement:

Mandatory Requirements

- 1.11.1. Ensure all necessary communication between Client, the triage team, and Security Researchers can be conducted via the platform (e.g. comments on reports, direct messages) in a secure manner.
- 1.11.2. Maintain a 24/7 emergency contact mechanism (phone or other agreed-upon channel) for critical vulnerability notifications requiring immediate attention. Escalation procedures and contact details (including backup contacts) must be provided to Client at program start.
- 1.11.3. Appoint a dedicated Customer Success Manager (as the primary program coordinator) and a Lead Triage Manager for Client's program. These individuals will serve as the main liaisons for operational discussions, issue resolution, and performance reviews. Service Provider shall provide Client with the names and qualifications (CVs) of these appointees before contract performance begins. Any changes in these key roles must be communicated in advance, and replacements must have equivalent expertise and familiarity with the program to ensure continuity.

Desirable, Non-Mandatory Requirements

None.

2. Obligations Regarding Security Researchers (Enforced by Service Provider)

Mandatory Requirements

To ensure the program's integrity and legal compliance, Service Provider shall be obliged to impose the requirements and rules as laid down in **Annex E** upon all participating Security Researchers. Furthermore, Service Provider shall be obliged to integrate equivalent terms and conditions on its platform.

Desirable, Non-Mandatory Requirements

None.

Annex C – Service Level Agreement (SLA)

1. Scope

This Service Level Agreement (SLA) defines the performance metrics, communication processes, and response times applicable to the Services provided by Service Provider under the Managed Bug Bounty Program as set out in the Framework Agreement and **Annex B** (Service Description and Requirements).

2. Triage Performance

Service Provider shall adhere to the following service levels for triage activities:

2.1. First Response Time

Service Provider shall acknowledge receipt of a new vulnerability submission within 2 hours of submission by the security researcher, preferably automatically.

2.2. Triage Completion Time

Service Provider shall complete validation and initial severity assessment of a submission within 3 business days of receipt.

Depending on the severity level, the following more strict maximum processing times apply:

- Exceptional (if applicable): Completion of validation within 1 business day
- Critical: Completion of validation within 1 business day
- High: Completion within 2 business days
- Medium: Completion within the standard 3 business days
- Low: Completion within the standard 3 business days

Any submission classified by Service Provider as Exceptional or Critical shall be escalated to Client immediately through the emergency contact mechanism in addition to being processed within the applicable triage completion time.

3. Communication with Security Researchers

All communication with Security Researchers shall be conducted exclusively via Service Provider's platform.

Service Provider shall make best efforts to ensure that all messages, inquiries, and status updates from Client and / or Security Researchers are responded to within 3 business hours.

When necessary, Client may be included in communications with Security Researchers, particularly in critical or disputed cases or in any event that requires a response to Security Researchers' questions.

4. Service Availability and Maintenance

The Service Provider shall ensure that the bug bounty platform, including all core functionalities required for submission, triage, and communication, maintains an availability of at least 99.9% per calendar month, excluding scheduled maintenance periods. Scheduled maintenance must

be communicated to the Client at least 48 hours in advance and should, where feasible, be conducted outside of Client's standard business hours.

In the event of unscheduled downtime or performance degradation affecting platform availability, the Service Provider shall notify the Client without undue delay providing an initial incident summary and an estimated time to resolution.

Where a platform incident, security incident, or service disruption may affect Client, Service Provider shall notify Client without undue delay and provide an initial incident summary, ongoing updates, and reasonable supporting information necessary for Client's internal assessment and any legal or regulatory response obligations.

5. Monitoring and Reporting

To ensure compliance with the above service levels, Service Provider will continuously monitor the relevant metrics. At least once a month, Service Provider will prepare an SLA report for Client. This report shall, as a minimum, include:

- Platform Availability
- Triage SLA Performance
- Submission Quality and Outcomes
- Bounty Pool Status
- Open Exceptional/Critical Submission

6. Service Level Breach

Repeated or significant failure to meet the agreed service levels may constitute a material breach of contract and entitle Client to take remedial action in accordance with Clause 8.3 of the Framework Agreement.

Annex D – List of In-Scope Systems and Assets

This **Annex D** defines the IT systems, applications, and digital Services that are explicitly authorised for testing under this Bug Bounty Program. Only the assets listed below are considered “in scope.” Testing any systems not listed here is strictly prohibited unless prior written authorisation is granted by Client.

1. General provisions

Testing is permitted only on the assets listed in this **Annex D**. Any testing outside the defined scope constitutes a breach of contract.

2. In-Scope Assets Overview

List of initial assets as applicable at the Effective Date (subject to change in accordance with Clause 4 of the Framework Agreement).

Testing is limited to the In-Scope Assets. The current list of In-Scope Assets is published on the Service Provider’s platform and includes:

- Mobile applications (iOS and Android)
- Mobile EUDI Wallet backend
- EUDI Hub web portal and backend
- PID provider backend

A more detailed technical scope, including where applicable domains, repositories, environments, and other technical identifiers, may be maintained by Client and implemented by Service Provider on the platform. The version of the in-scope asset list published on the platform, as approved in writing by Client, shall constitute the authoritative operational scope.

3. Out-of-Scope Assets and Activities

The following systems and activities are explicitly excluded from testing:

- Internal networks and non-public systems not listed in this **Annex D**
- Systems and applications operated by third parties (e.g. relying parties and issuers)
- Physical security testing
- Social engineering (e.g. phishing, vishing)
- (Distributed) Denial-of-Service (DoS/ DDoS) attacks

Furthermore, destructive testing or other high-risk methods are prohibited unless explicitly authorised in writing by Client.

Client intends to publish source code relating to the EUDI Wallet ecosystem as open source to the greatest extent reasonably possible. References to source code repositories in program documentation or on the bug bounty platform are provided for transparency and to assist researchers. However, vulnerability submissions are only considered in scope and eligible for triage and potential reward where the reported issue has an actual or reasonably demonstrable security impact on one or more of the expressly designated In-Scope Assets. Purely theoretical code findings, code quality concerns, or issues without such impact are not eligible for bounty payment and may be treated as out of scope.

Annex E – Vulnerability Disclosure Policy (VDP)

The VDP in this **Annex E** is to be implemented by Service Provider in accordance with Section 4.3. of the Framework Agreement and provide it to researchers.

Annex E constitutes the initial version of the VDP. The current binding version of the VDP shall be the version approved in writing by Client and published by Service Provider on the bug bounty platform. Service Provider shall not amend or publish changes to the VDP without Client's prior written approval.

1. Purpose and Scope

This Vulnerability Disclosure Policy (VDP) defines the rules of engagement, scope, and legal for Security Researchers participating in this Bug Bounty Program. The goal is to enable responsible disclosure of security vulnerabilities in systems operated by or on behalf of Client.

This policy applies to all In-Scope Assets as published on the Service Provider's platform.

2. In-Scope Assets

Testing is limited to the In-Scope Assets. The current list of In-Scope Assets is published on the Service Provider's platform and includes:

- Mobile applications (iOS and Android)
- Mobile EUDI Wallet backend
- EUDI Hub web portal and backend
- PID provider backend

Out-of-Scope Assets include systems operated by third parties (e.g., relying parties, issuers).

3. Permitted Testing Activities

Security Researchers are authorised to perform testing activities that comply with this policy and the Rules of Engagement. Permitted activities include:

- Non-destructive testing of In-Scope systems
- Testing within the defined scope and timeframes
- Use of non-intrusive techniques to identify vulnerabilities

Security Researchers must conduct their testing in good faith and in compliance with all applicable laws. This means they should not exploit any vulnerability beyond the extent necessary to demonstrate its existence, must not access, copy, or exfiltrate sensitive data (except what is minimally required for proof of concept).

4. Prohibited Activities

The following activities are strictly prohibited:

- Social engineering (e.g., phishing, vishing)
- Physical security testing (e.g., accessing offices or data centres)
- Attacks against third-party systems or Services
- Denial-of-Service (DoS/ DDoS) attacks
- Use of automated tools that generate excessive traffic or impact system availability

- Testing that could disrupt Services or compromise data integrity beyond what is necessary for finding vulnerability
- Accessing or modifying data that does not belong to you

5. Safe Harbor in favour of Service Provider and Security Researcher

Client assures that – provided Service Provider and Security Researchers act in good faith, within the scope of the Bug Bounty Program, and in full compliance with all Program rules (see Vulnerability Disclosure Policy, published on Service Providers website) – it will not initiate civil proceedings or file criminal complaints against those Security Researchers for their authorised security testing activities under the Program. This assurance is conditional upon the Security Researcher's adherence to the Program's terms and does not apply to any acts that exceed the authorised scope or violate the agreed rules. This Safe Harbor is a commitment by Client only and does not bind or limit the rights of any third party beyond Client's authorisation.

6. Reporting Process

Vulnerabilities must be reported via the Service Provider's platform using the secure submission form. Reports must include:

- A clear description of the vulnerability
- Steps to reproduce
- Impact assessment
- Any relevant technical evidence (e.g., logs, screenshots, PoC)

Reports must not be publicly disclosed without prior written consent from Client.

7. Confidentiality and Responsible Disclosure

Security Researchers are required to keep any vulnerability information discovered through the program strictly confidential until Client provides written permission to disclose it. They must not share details of vulnerabilities with any third parties, not even with other Security Researchers, outside the program's official communication channels. All Vulnerability Reports must be submitted privately via the designated platform. Public disclosure of vulnerability without consent, leaking exploit code, or sharing sensitive findings outside the program will lead to removal from the program and possible legal action.

8. Cooperation and Accountability

Security Researchers are expected to cooperate with Service Provider and Client in clarifying submissions when needed. If triage analysts or Client request additional information or steps to reproduce an issue, the Security Researcher should make a good faith effort to provide it. Security Researchers must also promptly comply with any instructions to halt testing on a particular asset or to destroy inadvertently accessed data. They should be aware that failure to follow the program's rules can result in removal from the program and forfeiture of any pending bounty rewards.

9. Legal Notice

By participating in the Program, researchers agree to the terms of this VDP and acknowledge that:

- This policy does not create a contractual relationship between the Security Researcher and Client.
- Participation is voluntary and does not entitle the researcher to compensation unless explicitly awarded under the bounty rules.
- Service Provider is the sole point of contact for all matters related to the Program.

10. Changes to this Policy

This policy may be updated from time to time by Client. The current version is published on Service Provider's platform.

Annex F – Pricing and Payment

1. Provider Fee

Tier	Maximum Annual Bounty To Spend	General Platform Fee (Annual) in Euro net	Triage Service Fee (Annual) in Euro net	Total Fee (= Sum of 'General Platform Fee' and 'Triage Service Fee') in Euro net
A	Up to €200,000			
B	Up to €300,000			
C	Up to €400,000			
D	Up to €500,000			
E	Up to €600,000			
F	Up to €700,000			
G	Up to €800,000			
H	Up to €900,000			
I	Up to €1,000,000			

2. Payment Process

- 2.1. All fees will be made in Euro net (any exchange rate risk shall be the sole responsibility of the Service Provider). For the avoidance of doubt, no Euro adjustments for any exchange rate fluctuations shall be applied.
- 2.2. Service Provider shall disburse all bounty rewards via a designated Trust Account, which it manages on behalf of Client.
- 2.3. Service Provider shall organize and administer the bounty payment process in an orderly fashion, including the applicable payment workflow and timeline (as set out in this **Annex F**).
- 2.4. Service Provider shall ensure that no bounty payment is released until the reported vulnerability has been duly validated and formally approved by Client.
- 2.5. Service Provider shall ensure that all bounty payments to eligible Security Researchers are executed promptly and securely.
- 2.6. Service Provider shall be able to administer bounty payments to eligible Security Researchers worldwide, including researchers located outside the European Union and the European Economic Area, provided that such payments are permitted under applicable law and successfully pass all required identity verification, tax compliance, anti-money-laundering, and sanctions-screening checks. Service Provider shall promptly inform Client of any country-specific payout restrictions that may materially limit researcher participation in the Program.

Annex G – Template Solution concept

As part of this tender, each bidder shall submit a written solution concept describing how the bidder intends to provide the Services in accordance with Annex B (Service Description and Requirements). The solution concept shall, for each subsection of Annex B, explain in a clear and sufficiently detailed manner how the bidder will implement the mandatory requirements and, where applicable, to what extent and in what manner the bidder can support the desirable, non-mandatory requirements. The document must not exceed 30 pages (excluding cover pages and table of contents) and must be formatted in font 11 (e.g. Arial or Calibri) or higher with standard margins (e.g. 2cm top/bottom/left/right). Any pages exceeding this limit will be ignored and not evaluated/considered.

It shall have the following structure:

1. Program Setup & Scope of Services (Annex B 1.1, 1.2)
2. Platform Capabilities & Integrations (Annex B 1.3, 1.4, 1.5)
3. Compliance, Governance & Security Management (Annex B 1.6)
4. Managed Triage Services (Annex B 1.7)
5. Researcher & Bounty Management (Annex B 1.8)
6. Analytics, Transparency & Reporting (Annex B 1.9)
7. Onboarding, Communication & Researcher Obligations (Annex B 1.10, 1.11, 2)

The evaluation will be carried out in accordance with this structure. This means that aspects relevant to the evaluation must be included in the relevant section. Consequently, if a tenderer presents, for example, aspects under point 1 that actually belong under point 2, these will not be taken into account under point 2.

Please note: The 'mandatory requirements' set out in the Annex B must always be met if the contract is awarded. Should your proposal deviate from these mandatory requirements, your bid will be rejected. Please therefore ensure that you do not deviate from these mandatory requirements – even inadvertently.

For details of the award criteria, please refer to Document B Award Criteria.

1. Program Setup & Scope of Services (Annex B 1.1, 1.2)

[to be filled out by the bidder]

2. Platform Capabilities & Integrations (Annex B 1.3, 1.4, 1.5)

[to be filled out by the bidder]

3. Compliance, Governance & Security Management (Annex B 1.6)

[to be filled out by the bidder]

4. Managed Triage Services (Annex B 1.7)

[to be filled out by the bidder]

5. Researcher & Bounty Management (Annex B 1.8)

[to be filled out by the bidder]

6. Analytics, Transparency & Reporting (Annex B 1.9)

[to be filled out by the bidder]

7. Onboarding, Communication & Researcher Obligations (Annex B 1.10, 1.11, 2)

[to be filled out by the bidder]

Annex H – Template CVs

Each CV shall not be longer than 3 pages and must be formatted in font 11 (e.g. Arial or Calibri) or higher with standard margins (e.g. 2cm top/bottom/left/right). Any pages exceeding this limit will be ignored and not evaluated/considered.

The bidder must clearly assign each CV to the relevant position (Customer Success Manager or Triage Team Manager). Please submit only these two CVs and no others. Please consider Part B Award Criteria regarding the CV aspects that will be evaluated. Only those aspects specified in Part B of the Award Criteria that are clearly stated in the CV will be assessed. You should therefore take care to prepare your CV in accordance with the requirements set out in Part B of the Award Criteria.

For details of the award criteria, please refer to Document B Award Criteria

FIRST NAME, LAST NAME			
Date of Birth	Current Job Title	Seniority Level	Employer
DD.MM.YYYY	XXX	XXX	XXX
Proposed Role in the Contract (please tick the relevant position)		<input type="checkbox"/> Customer Success Manager <input type="checkbox"/> Triage Team Manager	
Professional Profile <i>List your most relevant professional skills and strengths that are aligned with the proposed role.</i> <i>For Customer Success Manager:</i> <i>Please explain /demonstrate the expertise as required/evaluated according to the scoring table/evaluation in the document "Award criteria".</i> <i>For Triage Team Member:</i> <i>Please explain / demonstrate the expertise as required/evaluated according to the scoring table/evaluation in the document "Award criteria".</i>			
Language Skills <i>State your language skills (using the CEFR scale or another recognised standard).</i>			
EDUCATION/ TRAINING			
Year	Educational Institution	Field of Study / Training Programme	Degree / Qualification
MM.YYYY	XXX	XXX	M.Sc. / B.A. / Ph.D.
PROFESSIONAL EXPERIENCE (CHRONOLOGICAL)			
FROM - TO	Employer	Position	Description of Responsibilities and Performed Tasks

MM.YYYY – MM.YYYY	XXX	XXX	XXX
ADDITIONAL QUALIFICATIONS/ CERTIFICATIONS			
<i>Please list any additional qualifications or certifications that are relevant to the role</i>			

FIRST NAME, LAST NAME			
Date of Birth	Current Job Title	Seniority Level	Employer
DD.MM.YYYY	XXX	XXX	XXX
Proposed Role in the Contract (please tick the relevant position)		<input type="checkbox"/> Customer Success Manager <input type="checkbox"/> Triage Team Manager	
Professional Profile <i>List your most relevant professional skills and strengths that are aligned with the proposed role.</i> <i>For Customer Success Manager:</i> <i>Please explain /demonstrate the expertise as required/evaluated according to the scoring table/evaluation in the document "Award criteria".</i> <i>For Triage Team Member:</i> <i>Please explain / demonstrate the expertise as required/evaluated according to the scoring table/evaluation in the document "Award criteria".</i>			
Language Skills <i>State your language skills (using the CEFR scale or another recognised standard).</i>			
EDUCATION/ TRAINING			
Year	Educational Institution	Field of Study / Training Programme	Degree / Qualification
MM.YYYY	XXX	XXX	M.Sc. / B.A. / Ph.D.
PROFESSIONAL EXPERIENCE (CHRONOLOGICAL)			
FROM - TO	Employer	Position	Description of Responsibilities and Performed Tasks

MM.YYYY – MM.YYYY	XXX	XXX	XXX
ADDITIONAL QUALIFICATIONS/ CERTIFICATIONS			
<i>Please list any additional qualifications or certifications that are relevant to the role</i>			

Annex I – Data Processing Agreement and Standard Contractual Clauses

This Data Processing Agreement (“DPA”) is incorporated by reference into the Agreement governing the use of Processors services entered by and between Client (“Controller”) and Service Provider (“Processor”) to reflect the Parties’ agreement with regard to the Processing of Personal Data by Processor solely on behalf of the Controller. Each of the parties hereto may also be referred to as a “Party”, and together as the “Parties”.

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement. In the event of any conflict between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. Definitions

- 1.1. **Controller** – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- 1.2. **Personal Data** – any information relating to an identified or identifiable natural person (“Data Subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
- 1.3. **Personal Data Breach** – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed that is likely to result in a high risk to the rights and freedoms of natural persons.
- 1.4. **Processing** – any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated 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.
- 1.5. **Processor** – a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

2. Processing of Personal Data

2.1 Roles of the Parties.

This DPA applies when Personal Data is Processed by Processor as part of Processor’s provision of the Service, as further specified in the Agreement and any applicable order form. The Parties acknowledge and agree that with regard to the Processing of Personal Data on behalf

of Controller that is subject to the GDPR (i) Client is the Controller or Business, respectively, and (ii) Processor is the Processor or Service Provider, respectively.

2.2 Processor's Processing of Personal Data.

When Processing on Controller's behalf under or as required by the Agreement, Processor shall Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and as part of its provision of the Services; (ii) Processing to comply with Controller's other reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the Processing shall be performed.

2.3 Notwithstanding, Personal Data may be disclosed by Processor (a) if required by a subpoena or other judicial or administrative order, or if otherwise required by law; or (b) if Processor deems the disclosure necessary to protect the safety and rights of any person, or the public.

2.4 Processor shall inform Controller without undue delay if, in Processor's opinion, an instruction for the Processing of Personal Data given by Controller infringes applicable Data Protection Laws. To the extent that Processor cannot comply with an instruction from Controller, (i) Processor shall inform Controller, providing relevant details of the issue, (ii) Processor may, without liability to Controller, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) or suspend Controller's access to the Services

2.5 Details of the Processing.

The subject matter of Processing of Personal Data by Processor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of Processing) to this DPA.

2.6 CPRA Standard of Care; No Sale of Personal Information.

Processor will not (1) sell (as defined in the CPRA or other Data Protection Laws) Personal Data, or (2) retain, use or disclose Personal Data: (i) for any purpose other than for the specific purpose of performing the Subscription Services, (ii) outside of the direct business relationship between Controller and Processor, except as permitted under applicable Data Protection Laws, or (3) combine Personal Data received pursuant to the Agreement with personal information (as defined in the CPRA) (i) received from or on behalf of another person, or (ii) collected from Processor's own interaction with any Data Subject to whom such Personal Data pertains. Processor does not receive any Personal Data from Controller as consideration for its provision of Subscription Services. Processor certifies that it understands the restrictions set forth in this Section and will comply with them.

3. Data subject requests

If Processor receives a request from a Data Subject or Consumer, regulator, or supervisory authority to exercise their rights under applicable Data Protection Laws "Data Subject Request"), the Processor shall, to the extent legally permitted, notify or refer the Data Subject or authority to the Controller without undue delay and, in any event, no later than three (3) days

after receipt of such request. The Parties shall, upon request, promptly provide each other with reasonable assistance and information necessary to enable the other Party to respond to and comply with such requests or the exercise of such rights. Considering the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organizational measures, insofar as possible and reasonable, for the fulfilment of Controller's obligation to respond to a Data Subject. Where appropriate, Processor may advise Data Subjects on available features for self-exercising their Data Subject Requests through the Services or refer Data Subject Requests directly to the Controller for handling.

4. Confidentiality

Processor shall ensure that its personnel and advisors engaged in the Processing of Personal Data (i) are contractually bound to confidentiality requirements no less than what is required under this DPA and (ii) are informed of the confidential nature of Personal Data and required to keep it confidential.

5. Sub-Processors

The Processor shall comply with the following obligations when it uses a third party for the purposes of the Processing:

- The Processor shall be responsible and liable for the acts, omissions or defaults of its Subcontractors in the performance of obligations under this Agreement or otherwise as if they were its own acts, omissions or defaults.
- The Processor shall guarantee the Controller that the subcontracting shall not affect in any manner its compliance with the applicable Data Protection Laws (and notably Controller's obligation to promptly respond to requests for access, modification, deletion, opposition, portability and limitation of Processing or any requests from persons whose Personal Data is subject to Processing).
- The Processor shall ensure that third parties it may use are bound by the same obligations as itself in terms of Personal Data Processing and protection and, in particular, those provided in this Agreement, and/or those provided in Processor other instructions and/or those provided in the applicable Data Protection Laws, and at no expense for the Controller, the Processor shall actively (i) monitor, regularly verify and, if applicable, take all measures such that the Subcontractors comply with their obligations, and (ii) promptly notify the Controller of any non-compliance detected by it or which has been reported to it and all measures it has taken to remedy such non-compliance.
- In case of sub Processing to any subcontractor located outside the EEA in a country that is not recognized as providing an adequate level of data protection, the Processor will provide the Controller with information and relevant documentation on the mechanism for international data transfers pursuant to Art. 46 of the GDPR that is used to lawfully disclose its Personal Data to the subcontractor. Processor shall not engage any Sub-processor without the prior authorization of the Controller.

- The Processor shall inform the Controller in writing of any intended engagement or replacement of a Sub-processor at least fourteen (14) days in advance. Such notification shall include all information necessary for the Controller to assess the impact of the proposed Sub-processor.
- The Controller may object to the proposed engagement of a Sub-processor within fourteen (14) days of receipt of the notification for reasonable data protection grounds.
- If the Controller does not object within this period, the Controller's authorization shall be deemed to have been granted.

6. Security & Audits

The Processor shall enable the Controller and its representatives to carry out any audit of Processor's Processing activities, including by accessing Processor's facilities to verify that the Processor complies with its obligations provided in the Agreement, pursuant to Controller's instructions and the applicable Data Protection Laws.

The Controller shall have the right to audit the Processor only during business hours and in such manner that the audit does not interfere with Processor's normal activity.

7. Data Incident Management and Notification

Processor maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Controller without undue delay (maximum 24hrs) after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by Processor on behalf of the Controller (a "Data Incident"). Processor's notice will at least: (a) describe the nature of the Data Incident including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) communicate the name and contact details of Processor's data protection team, which will be available to provide any additional Data Incident; (c) describe the measures taken or proposed to be taken by Processor to address the Data Incident, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. Processor shall document any such Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken.

8. Return and deletion of Personal Data

Within 90 days following termination of the Agreement and subject thereto, Processor shall, at the choice of Controller (indicated through the Services or in written notification to Processor), delete or return to Controller all the Personal Data it Processes solely on behalf of the

Controller in the manner described in the Agreement, and Processor shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, Processor may also retain one copy of the Personal Data as necessary for routine backup, archiving, evidence purposes, legal claims, or compliance with legal obligations.

9. Cross-border data transfers

9.1 Transfers from the EEA, Switzerland and the United Kingdom to countries that offer adequate level or data protection. Personal Data may be transferred from EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) (collectively, “EEA”), Switzerland and the United Kingdom (“UK”) to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, Switzerland, or the UK as relevant, as applicable, without any further safeguard being necessary.

9.2 The Parties acknowledge that, under the MSA, U.S. Controller transfers all data, including Personal Data, to Processor within the United States and that U.S. Controller may have received data, including Personal Data, from its various European subsidiaries through lawful mechanisms of transfer, including under the GDPR. The Parties further acknowledge that the data flow between the Parties takes place entirely within the United States. Processor will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws and Regulations.

9.3 Processor will (i) provide at least the same level of privacy protection as required by the EU-U.S. Data Privacy Framework Principles; (ii) notify Controller if Processor makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) upon notice, including under the preceding sub-section (ii), take reasonable and appropriate steps to remediate unauthorized Processing.

9.4 The parties agree that when the transfer of Personal Data from Controller to Processor is a Restricted Transfer, such Restricted Transfer will be subject to the clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“EU SCCs”), which are deemed incorporated and for a part of this DPA as follows:

9.4.1 In relation to Restricted Transfers of Controller’s Personal Data protected by the GDPR, the EU SCCs will apply, completed as follows:

- (i) the module specified in Schedule 2 will apply;
- (ii) In Clause 7, the optional docking clause will apply.
- (iii) In Clause 9, Option 2 will apply, and the time period for prior notice of sub-Processor changes will be as set out in Section 5 of this DPA.
- (iv) In Clause 11, the optional language will not apply.

(v) In Clause 17, Option 1 will apply, and the EU SCCs will be governed by German law.

(vi) In clause 18(b), disputes will be resolved before the courts of Germany.

9.4.2 In order to safeguarding EEA Transferred Data, when any government or regulatory agency of a Third Country (“Authority”) requests access to such data (“Request”), and unless required by a valid court order or if otherwise Processor may face criminal charges for failing to comply with orders or demands to disclose or otherwise provide access to EEA Transferred Data, or where the access is requested in the event of imminent threat to lives, Processor will:

(i) not allow access to EEA Transferred Data, for example by providing any Authority with encryption keys; and

(ii) upon Controller’s written request, provide reasonable available information about the requests of access to Personal Data by government agencies that Processor has received in the six (6) months preceding to Controller’s request.

9.4.3 If Processor receives a Request, Processor will notify Controller of such request to enable the Controller to take necessary actions, to communicate directly with the relevant agency and to respond to the Request. If Processor is prohibited by law to notify the Controller of the Request, Processor will make reasonable efforts to challenge such prohibition through judicial action or other means at Controller’s expense and, to the extent possible, will provide only the minimum amount of information necessary.

9.4.4 In relation to transfers of UK GDPR-governed Personal Data (“UK Transferred Data”) to a Third Country, the EU SCCs: (i) apply as completed in accordance with sections 9.2 and 9.3 above; and (ii) are deemed amended as specified by the UK Addendum, which is deemed executed by the parties and incorporated into and forming an integral part of this DPA.

9.4.5 In relation to Restricted Transfers of Controller’s Personal Data that is subject to the Swiss FDPA (“Swiss Transferred Data”), the following modifications shall apply to the EU SCCs to the extent that the Swiss FDPA applies to Processor’s Processing of Controller’s Personal Data: (a) the term “member state” as used in the EU SCCs will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs; (b) references to the GDPR or other governing law contained in the EU SCCs shall also be interpreted to include the Swiss FDPA; and (c) the parties agree that the supervisory authority as indicated in Annex I.C of the EU SCCs shall be the Swiss Federal Data Protection and Information Commissioner.

9.4.6 The terms set forth in Part 2 of Schedule 2 (Additional Safeguards) shall apply to an EEA Transfer and a UK Transfer.

10. Liability

The liability of the parties shall be governed by the applicable statutory provisions, in particular Article 82 of the GDPR.

11. Other provisions

11.1 Data Protection Impact Assessment and Prior Consultation. Upon Controller's reasonable request, Processor shall provide Controller, at Controller's cost, with reasonable cooperation and assistance needed to fulfil Controller's obligation under the GDPR or the UK GDPR (as applicable) to carry out a data protection impact assessment related to Controller's use of the Services, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide, reasonable assistance to Controller in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 12.1, to the extent required under the GDPR, as applicable.

Appendix 1 to Annex I – Details of the Processing

1. Nature and Purpose of Processing

[...]

2. Duration of Processing

[...]

3. Type of Personal Data

[...]

4. Categories of Data Subjects

[...]

5. Categories of Personal Data processed

[...]

Appendix 2 to Annex I – Technical and Organizational Measures including Technical and Organisational Measures to ensure the security of the data

EXPLANATORY NOTE:

The following technical and organisational measures apply to all processing of Personal Data carried out by the Processor on behalf of the Controller under the Data Processing Agreement. The measures described below specifically address the processing activities arising in the context of the managed bug bounty platform operated by the Processor, including the processing of Security Researcher personal data (including identity, contact, and payment information), vulnerability reports, bounty transaction records, and platform access and authentication data.

Technical and organisational measures	Technical and organisational measures
Encryption How is encryption guaranteed? Encryption transforms plain text into an associated ciphertext (ciphertext) depending on additional information called a "key", which should be indecipherable for those who do not know the key.	<input type="checkbox"/> Encryption techniques for notebooks <input type="checkbox"/> Where appropriate and possible, personal data is replaced by random codes / pseudonymised <input type="checkbox"/> Personal data is encrypted during electronic transmission outside of secure networks
Ability to maintain confidentiality How is data confidentiality guaranteed in the long term? Confidentiality means that personal data is protected against unauthorised disclosure.	Access control <input type="checkbox"/> Alarm systems <input type="checkbox"/> Regulations on the loss of ID cards <input type="checkbox"/> Centralised electronic locking system <input type="checkbox"/> Special structural precautions (e.g. grilles, opaque panes, screens, room dividers) <input type="checkbox"/> Regulations for the supervision of service personnel <input type="checkbox"/> Escape routes and gates/doors (e.g. supplier entrances) <input type="checkbox"/> Window locks <input type="checkbox"/> All doors and gates can only be opened after an authorisation check <input type="checkbox"/> Regulations for the admission of external persons (e.g. customers, guests, suppliers) <input type="checkbox"/> Regulations on access to separate spatial areas <input type="checkbox"/> Logging who has visited which specific premises and when <input type="checkbox"/> Regulations for the presence of third parties in special premises <input type="checkbox"/> Service personnel (e.g. cleaning service, maintenance personnel) for special premises are carefully selected and bound by data protection laws <input type="checkbox"/> Authorisation concept

	<input type="checkbox"/> Regulation on the allocation, administration and withdrawal of access authorisations <input type="checkbox"/> Access only possible with user ID and password <input type="checkbox"/> Access only with strong authentication MFA (multi-factor authentication) <input type="checkbox"/> Limitation of login attempts <input type="checkbox"/> Blocking in the event of prolonged inactivity <input type="checkbox"/> Firewall <input type="checkbox"/> Intrusion detection/prevention systems <input type="checkbox"/> Virus protection programmes <input type="checkbox"/> Regulations for substitutions and absences <input type="checkbox"/> Logging of anomalies (e.g. unsuccessful login attempts) <input type="checkbox"/> Logging/detection of intrusion attempts into the company network <input type="checkbox"/> No internal network in public areas <input type="checkbox"/> Penetration test
<p>Ability of integrity</p> <p>How is the ability to ensure the integrity of the data permanently guaranteed?</p> <p>Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is applied to "data", it means that the data is complete and unchanged.</p>	<input type="checkbox"/> Access authorisations are function- and position-dependent ("need to know"), especially for extended authorisations (e.g. administrator IDs) <input type="checkbox"/> Identity management ensures that no unwanted/critical side effects arise from the assignment of different authorisations <input type="checkbox"/> Separation of test and production operations <input type="checkbox"/> Internal specifications for data separation <input type="checkbox"/> Free database queries are limited <input type="checkbox"/> Regulations on the storage of mobile data carriers (USB sticks, DVDs, CDs, memory cards, etc.) <input type="checkbox"/> Regulations on the disposal of data storage media (hard drives, tapes, DVDs, CDs, USB sticks, memory cards, etc.) in compliance with data protection regulations <input type="checkbox"/> Regulations for copying data sets to data carriers (especially for particularly sensitive personal data, Art. 9 GDPR) <input type="checkbox"/> Regulations on the storage of backup copies (access mechanisms must also work with backup copies) <input type="checkbox"/> Techniques that prevent the alteration of electronically transmitted data or at least make this recognisable (e.g. digital signature) <input type="checkbox"/> It is defined to which location which personal data is transferred by means of data carrier transport. Only the specified data transports are carried out

<p>Availability capability</p> <p>How is the ability to make data permanently available guaranteed?</p> <p>The availability of services, functions of an IT system, IT applications or IT networks or even information is ensured if these can always be used by users as intended.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> The location of the buildings is chosen so that the service can be provided properly under normal circumstances (e.g. the buildings are not located in a flood zone) <input type="checkbox"/> Power supply (UPS) is secured <input type="checkbox"/> Firewall and virus scanner <input type="checkbox"/> Climate control in the data centre (temperature, humidity) <input type="checkbox"/> System maintenance work is only carried out by qualified specialists <input type="checkbox"/> Vulnerability analysis for the operation of the data centre <input type="checkbox"/> Emergency plan, emergency management and regular tests <input type="checkbox"/> Fire protection measures (e.g. smoke detectors, extinguishing system, fire extinguishers) <input type="checkbox"/> Protection against water ingress <input type="checkbox"/> Capacity management <input type="checkbox"/> Vulnerability management
<p>Ability to work under pressure</p> <p>How is the resilience of the data guaranteed in the long term?</p> <p>Systems are resilient if they are so robust that they can function even under heavy access or heavy utilisation.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Ensured sufficient reserve capacities <input type="checkbox"/> Patch management <input type="checkbox"/> Load tests (load/volume/stress tests) and other performance tests on system response times
<p>Recoverability of availability and access</p> <p>How is it ensured that personal data is quickly available and accessible again after security incidents?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Data backup concept that ensures rapid recovery <input type="checkbox"/> All relevant data is backed up regularly <input type="checkbox"/> Documentation on the number and location of the respective backup copies <input type="checkbox"/> Regulations for the handling and storage of backup copies <input type="checkbox"/> The restoration of backed-up data is tested
<p>Procedure for regular review</p> <p>How is it ensured that the aforementioned data backup measures are regularly reviewed?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> There is a defined test routine <input type="checkbox"/> Test reports are evaluated <input type="checkbox"/> Implementation of suggestions for improvement <input type="checkbox"/> Annual tests

<p>Unlawful access to personal data</p> <p>How can data processing systems be prevented from being used by unauthorised persons?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Regulations on the assignment, administration and revocation of access authorisations <input type="checkbox"/> Regulations for the use of passwords (e.g. restricted duration, minimum length, complexity/special characters) <input type="checkbox"/> Regulations for access to systems from outside <input type="checkbox"/> Rules for leaving the workplace (clean desk) <input type="checkbox"/> Regulations on the persons authorised to transfer data by means of data carriers <input type="checkbox"/> Regulations for the transport of data carriers (e.g. only in sealed containers) <input type="checkbox"/> Personal data on data carriers is encrypted during transport <input type="checkbox"/> Regulations that data carriers are only stored in secure environments (e.g. locked cabinets, safes) <input type="checkbox"/> Regulations on when and how to dispose of data carriers
<p>Processing of personal data only according to instructions</p> <p>How is it ensured that personal data is only processed in accordance with the controller's instructions?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Employees are bound by rules of conduct <input type="checkbox"/> Implementation of internal company data protection guidelines <input type="checkbox"/> Obligation of employees to maintain data secrecy <input type="checkbox"/> Regular training for all employees with access authorisation <input type="checkbox"/> Determination of contact persons and responsible project managers for the specific order

Appendix 3 to Annex I – Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of personal data to a third country.
 - (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A (hereinafter each “data exporter”), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each “data importer”)
- have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
 - (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing Services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of

sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational

measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) 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.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
 - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of

destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

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]*

1. Name: ...

Address: ...

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

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

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

1. Name: ...

Address: ...

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

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

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.

.....

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

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

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

.....

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

.....

C. COMPETENT SUPERVISORY AUTHORITY

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

.....

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Technical and organisational measures	Technical and organisational measures
Encryption How is encryption guaranteed? Encryption transforms plain text into an associated ciphertext (ciphertext) depending on additional information called a "key", which should be indecipherable for those who do not know the key.	<input type="checkbox"/> Encryption techniques for notebooks <input type="checkbox"/> Where appropriate and possible, personal data is replaced by random codes / pseudonymised <input type="checkbox"/> Personal data is encrypted during electronic transmission outside of secure networks
Ability to maintain confidentiality How is data confidentiality guaranteed in the long term? Confidentiality means that personal data is protected against unauthorised disclosure.	Access control <input type="checkbox"/> Alarm systems <input type="checkbox"/> Regulations on the loss of ID cards <input type="checkbox"/> Centralised electronic locking system <input type="checkbox"/> Special structural precautions (e.g. grilles, opaque panes, screens, room dividers) <input type="checkbox"/> Regulations for the supervision of service personnel <input type="checkbox"/> Escape routes and gates/doors (e.g. supplier entrances) <input type="checkbox"/> Window locks <input type="checkbox"/> All doors and gates can only be opened after an authorisation check <input type="checkbox"/> Regulations for the admission of external persons (e.g. customers, guests, suppliers) <input type="checkbox"/> Regulations on access to separate spatial areas <input type="checkbox"/> Logging who has visited which specific premises and when <input type="checkbox"/> Regulations for the presence of third parties in special premises <input type="checkbox"/> Service personnel (e.g. cleaning service, maintenance personnel) for special premises are carefully selected and bound by data protection laws

	<input type="checkbox"/> Authorisation concept
	<input type="checkbox"/> Regulation on the allocation, administration and withdrawal of access authorisations <input type="checkbox"/> Access only possible with user ID and password <input type="checkbox"/> Access only with strong authentication MFA (multi-factor authentication) <input type="checkbox"/> Limitation of login attempts <input type="checkbox"/> Blocking in the event of prolonged inactivity <input type="checkbox"/> Firewall <input type="checkbox"/> Intrusion detection/prevention systems <input type="checkbox"/> Virus protection programmes <input type="checkbox"/> Regulations for substitutions and absences <input type="checkbox"/> Logging of anomalies (e.g. unsuccessful login attempts) <input type="checkbox"/> Logging/detection of intrusion attempts into the company network <input type="checkbox"/> No internal network in public areas <input type="checkbox"/> Penetration test
Ability of integrity <p>How is the ability to ensure the integrity of the data permanently guaranteed?</p> <p>Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is applied to "data", it means that the data is complete and unchanged.</p>	<input type="checkbox"/> Access authorisations are function- and position-dependent ("need to know"), especially for extended authorisations (e.g. administrator IDs) <input type="checkbox"/> Identity management ensures that no unwanted/critical side effects arise from the assignment of different authorisations <input type="checkbox"/> Separation of test and production operations <input type="checkbox"/> Internal specifications for data separation <input type="checkbox"/> Free database queries are limited <input type="checkbox"/> Regulations on the storage of mobile data carriers (USB sticks, DVDs, CDs, memory cards, etc.) <input type="checkbox"/> Regulations on the disposal of data storage media (hard drives, tapes, DVDs, CDs, USB sticks, memory cards, etc.) in compliance with data protection regulations <input type="checkbox"/> Regulations for copying data sets to data carriers (especially for particularly sensitive personal data, Art. 9 GDPR) <input type="checkbox"/> Regulations on the storage of backup copies (access mechanisms must also work with backup copies) <input type="checkbox"/> Techniques that prevent the alteration of electronically transmitted data or at least make this recognisable (e.g. digital signature) <input type="checkbox"/> It is defined to which location which personal data is transferred by means of data carrier transport. Only the specified data transports are carried out

<p>Availability capability</p> <p>How is the ability to make data permanently available guaranteed?</p> <p>The availability of services, functions of an IT system, IT applications or IT networks or even information is ensured if these can always be used by users as intended.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> The location of the buildings is chosen so that the service can be provided properly under normal circumstances (e.g. the buildings are not located in a flood zone) <input type="checkbox"/> Power supply (UPS) is secured <input type="checkbox"/> Firewall and virus scanner <input type="checkbox"/> Climate control in the data centre (temperature, humidity) <input type="checkbox"/> System maintenance work is only carried out by qualified specialists <input type="checkbox"/> Vulnerability analysis for the operation of the data centre <input type="checkbox"/> Emergency plan, emergency management and regular tests <input type="checkbox"/> Fire protection measures (e.g. smoke detectors, extinguishing system, fire extinguishers) <input type="checkbox"/> Protection against water ingress <input type="checkbox"/> Capacity management <input type="checkbox"/> Vulnerability management
<p>Ability to work under pressure</p> <p>How is the resilience of the data guaranteed in the long term?</p> <p>Systems are resilient if they are so robust that they can function even under heavy access or heavy utilisation.</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Ensured sufficient reserve capacities <input type="checkbox"/> Patch management <input type="checkbox"/> Load tests (load/volume/stress tests) and other performance tests on system response times
<p>Recoverability of availability and access</p> <p>How is it ensured that personal data is quickly available and accessible again after security incidents?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Data backup concept that ensures rapid recovery <input type="checkbox"/> All relevant data is backed up regularly <input type="checkbox"/> Documentation on the number and location of the respective backup copies <input type="checkbox"/> Regulations for the handling and storage of backup copies <input type="checkbox"/> The restoration of backed-up data is tested
<p>Procedure for regular review</p> <p>How is it ensured that the aforementioned data backup measures are regularly reviewed?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> There is a defined test routine <input type="checkbox"/> Test reports are evaluated <input type="checkbox"/> Implementation of suggestions for improvement <input type="checkbox"/> Annual tests

<p>Unlawful access to personal data</p> <p>How can data processing systems be prevented from being used by unauthorised persons?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Regulations on the assignment, administration and revocation of access authorisations <input type="checkbox"/> Regulations for the use of passwords (e.g. restricted duration, minimum length, complexity/special characters) <input type="checkbox"/> Regulations for access to systems from outside <input type="checkbox"/> Rules for leaving the workplace (clean desk) <input type="checkbox"/> Regulations on the persons authorised to transfer data by means of data carriers <input type="checkbox"/> Regulations for the transport of data carriers (e.g. only in sealed containers) <input type="checkbox"/> Personal data on data carriers is encrypted during transport <input type="checkbox"/> Regulations that data carriers are only stored in secure environments (e.g. locked cabinets, safes) <input type="checkbox"/> Regulations on when and how to dispose of data carriers
<p>Processing of personal data only according to instructions</p> <p>How is it ensured that personal data is only processed in accordance with the controller's instructions?</p>	<ul style="list-style-type: none"> <input type="checkbox"/> Employees are bound by rules of conduct <input type="checkbox"/> Implementation of internal company data protection guidelines <input type="checkbox"/> Obligation of employees to maintain data secrecy <input type="checkbox"/> Regular training for all employees with access authorisation <input type="checkbox"/> Determination of contact persons and responsible project managers for the specific order

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...