Data Processing Agreement (DPA)

Entered into pursuant to Article 28 of Regulation (EU) 2016/679 ("GDPR"), supplemented by an annex addressing Article 30 of Regulation (EU) 2022/2554 ("DORA")

Version 1.1 — **[TO BE COMPLETED: effective date]**

Between the parties

The Customer

- Legal name: **[TO BE COMPLETED: Customer's legal name]**
- Legal form and register: **[TO BE COMPLETED]**
- Registered office: **[TO BE COMPLETED]**
- Represented by: **[TO BE COMPLETED: name, title]**
- Compliance / data protection contact (notifications under Sections 5.4.2 and 5.6): **[TO BE COMPLETED: email address]**

hereinafter "**the Customer**", acting as **controller** or, where applicable, as a first-tier processor acting on behalf of its own controller clients (Section 6.2),

and

Cryptaguard BV, a private limited company (BV) incorporated under Belgian law

- Company number (CBE): 1007.610.660
- Registered office: Fazantenlaan 9, 1600 Sint-Pieters-Leeuw, Belgium
- Represented by: Matthieu Roland, director

operating the **ResiPlan** software platform (the "**Service**"), hereinafter "**the Processor**",

together "the **Parties**".

---

1. Definitions

The terms "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meanings given to them in Article 4 GDPR. The terms "financial entity", "ICT third-party service provider" and "critical or important function" have the meanings given to them in Article 3 of DORA. "Main Agreement" means the terms of service of the Service accepted by the Customer **[TO BE COMPLETED: reference and version of the ToS/services agreement]**, which this agreement supplements.

2. Subject matter and order of precedence

2.1. This agreement (the "**DPA**") governs the processing of personal data carried out by the Processor **on behalf of the Customer** in the course of providing the Service, in accordance with Article 28 GDPR.

2.2. The DPA forms an integral part of the Main Agreement. In the event of a conflict between the DPA and the Main Agreement regarding the processing of personal data, the DPA prevails.

2.3. Where the Customer is a financial entity within the meaning of DORA, or acts on behalf of a financial entity, **Annex 5** sets out the contractual provisions required by Article 30 of DORA and

prevails, for those matters, over any less protective provision.

2.4. The obligations and rights of the Customer, in its capacity as controller, are defined by this DPA — in particular Sections 5.1 (instructions), 5.4.2 (objection to sub-processors), 5.8 (choice as to return or deletion), 5.9 (audits) and 6 — as well as by the Main Agreement.

3. Description of the processing

The detailed description of the processing — subject matter, duration, nature and purposes, categories of personal data and categories of data subjects — is set out in **Annex 1**, in accordance with Article 28(3) GDPR.

4. Term

The DPA applies for as long as the Processor processes personal data on behalf of the Customer, and at the latest until expiry of the deletion period provided for in Section 5.8.

5. Obligations of the Processor

5.1. Documented instructions

The Processor processes personal data **only on documented instructions from the Customer**, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law; in such a case, the Processor informs the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Main Agreement, the Customer's configuration of the Service and this DPA constitute the initial documented instructions. The Processor immediately informs the Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

5.2. Confidentiality

The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and process the data only on instructions and as needed for their duties.

5.3. Security of processing

The Processor implements the technical and organisational measures described in **Annex 2**, in accordance with Article 32 GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons. The Processor may update these measures, provided the overall level of protection is not reduced.

5.4. Sub-processing

5.4.1. The Customer grants the Processor a **general written authorisation** to engage the sub-processors listed in **Annex 3**.

5.4.2. The Processor informs the Customer of any intended (i) addition or replacement of a sub-processor, or (ii) **change of the locations** (regions or countries) of service provision or of data processing/storage listed in Annexes 3 and 4 — including where an existing sub-processor changes

location — **at least 30 days** before it takes effect. Notification is sent by email to the compliance contact designated above, in addition to a notification to the administrators of the Customer's organisation and an update of the public transparency page; the objection period runs from the email. Where the Customer has declared that it acts on behalf of a third-party controller or financial entity, the notice period is extended to **60 days** so as to preserve a usable cascading objection window. The Customer may raise legitimate, documented objections within that period; failing agreement on a reasonable alternative, the Customer may terminate the Main Agreement in respect of the affected part of the Service, without penalty and with a pro-rata refund of prepaid fees for the unused period.

5.4.3. The Processor imposes on each sub-processor, by way of contract, data protection obligations **at least equivalent** to those of this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures. The Processor remains **fully liable** to the Customer for the performance of the sub-processors' obligations.

5.5. Assistance — data subject rights

Taking into account the nature of the processing, the Processor assists the Customer by appropriate technical and organisational measures in fulfilling its obligation to respond to requests for the exercise of data subject rights (Articles 12 to 23 GDPR: access, rectification, erasure, restriction, portability, objection). The Service enables the Customer to view, rectify, export and delete data itself; for any request requiring the Processor's intervention, the Processor responds within a maximum of **10 business days**. If a data subject contacts the Processor directly, the Processor forwards the request to the Customer without undue delay and does not respond itself, unless otherwise instructed by the Customer.

5.6. Notification of personal data breaches and ICT incidents

5.6.1. **Personal data breaches.** The Processor notifies the Customer of any personal data breach **without undue delay and at the latest [TO BE CONFIRMED: 24] hours** after becoming aware of it, at the address of the compliance contact designated above. To the extent information is available, the notification contains the elements set out in Article 33(3) GDPR: nature of the breach, categories and approximate number of data subjects and records concerned, likely consequences, measures taken or proposed, and a contact point. The Processor documents the breach and cooperates with the Customer for any notification to the supervisory authority or communication to data subjects.

5.6.2. **ICT incidents.** Independently of any personal data breach, the Processor notifies the Customer, without undue delay and at the latest **[TO BE CONFIRMED: 24] hours** after becoming aware of it, of any ICT-related incident affecting the Service, with the information necessary for its classification by the Customer under DORA: affected scope, observed or estimated impact, chronology, remediation measures undertaken, and a contact point. The Processor keeps the Customer informed until resolution.

5.6.3. Notification of a breach or incident shall not be construed as an acknowledgement of fault or liability.

Processor's notification contact: security@resiplan.eu

5.7. Assistance — security, DPIA and prior consultation

The Processor assists the Customer in ensuring compliance with the obligations set out in Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to it, in particular for data protection impact assessments (DPIA) and prior consultation of the supervisory

authority. The Service's security documentation (Annex 2, privacy policy, trust center) is provided for this purpose at no additional cost.

5.8. Return and deletion of data

5.8.1. Throughout the term of the Main Agreement, as well as during the transition period provided for in Annex 5 (30(3)(f)) and in the event of the Processor's insolvency, resolution or discontinuation of business, the Customer may **export at any time** all of its data — **personal and non-personal** (impact analyses, plans, registers, mappings, documents) — using the Service's export functions (PDF, Excel/CSV, DOCX) and through the API (JSON).

5.8.2. Upon termination of the Main Agreement, the Processor, **at the choice of the Customer**, deletes all data or returns it to the Customer in a structured, commonly used and easily accessible format, and destroys existing copies, unless Union or Member State law requires their retention. In the absence of instructions from the Customer within **[TO BE CONFIRMED: 30] days** of termination, the Processor proceeds with deletion; where the Customer is a financial entity that has notified CIF status (Annex 5), no default deletion occurs before the end of the transition period **and** written confirmation. Backups are deleted at the latest **[TO BE CONFIRMED: 35] days** after deletion of production data. Upon request, the Processor certifies deletion in writing.

5.9. Audits and demonstration of compliance

5.9.1. The Processor makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. Due diligence questionnaires and documentary reviews do not count towards the frequency limit below.

5.9.2. The Processor allows for and contributes to **audits, including inspections**, conducted by the Customer or a third-party auditor mandated by the Customer (not a competitor of the Processor, and bound by confidentiality). Except in the event of an established breach, a security incident affecting the Customer, a reasonable and documented suspicion of non-compliance, or a requirement of a supervisory authority, such audits are limited to **one per twelve-month period**, upon **30 days'** prior written notice, during business hours, without disproportionately disrupting the operation of the Service, each Party bearing its own costs.

5.9.3. Where the Customer is a financial entity (or acts on behalf of one), the **extended access, inspection and audit rights provided for in Annex 5 (DORA)** apply in addition and prevail in the event of a conflict.

5.10. Crisis session recordings

Where the Customer enables the recording of crisis sessions: (i) transcription is performed **locally by default**, on the Processor's infrastructure in the European Union; use of the cloud provider listed in Annex 3 requires explicit activation by the Customer's organisation; (ii) audio files and transcripts are subject to a retention period configurable by the Customer; (iii) access to them is restricted to the authorised roles of the Customer's organisation; (iv) the Customer is responsible for informing participants of the recording beforehand, in accordance with Articles 13 and 14 GDPR.

6. Obligations of the Customer

6.1. The Customer warrants that the entrusted processing rests on a valid legal basis, that the data was collected lawfully, that data subjects have been informed in accordance with Articles 13 and 14 GDPR, and that its instructions comply with applicable law. The Customer is responsible for the configuration of

the Service (including account, role and permission management, and activation of optional features) and for the accuracy of the data it enters.

6.2. **Processing chain.** Where the Customer acts as a processor on behalf of a controller, it warrants that: (i) it has obtained that controller's prior written authorisation, specific or general, to engage the Processor, in accordance with Article 28(2) GDPR; (ii) the obligations imposed on the Processor by this DPA are at least equivalent to those of its own processing contract, in accordance with Article 28(4); (iii) it will pass on to the controller without delay the notifications received under Sections 5.4.2 and 5.6.

6.3. **Special categories of data (Art. 9 GDPR).** The Service is not intended for the **systematic or structured** processing of special categories of data, which remains prohibited without the Processor's prior written agreement. Incidental mentions of such data in free-text content (incident reports, exercise records, crisis session recordings) are covered by this DPA and benefit from the measures of Annex 2; the Customer ensures their minimisation and determines, in its capacity as controller, their legal basis.

7. International transfers

Transfers of personal data to third countries or to international organisations are governed by Chapter V GDPR, under the conditions described in **Annex 4**. The Processor carries out no unlisted transfer without following the procedure in Section 5.4.

8. Liability and insurance

8.1. Each Party's liability under this DPA is governed by the liability regime of the Main Agreement, subject to the following: for breaches of this DPA and incidents affecting the security or confidentiality of the Customer's data, the Processor's liability is capped at **[TO BE COMPLETED: dedicated cap — e.g. twice the annual fees]**, by way of derogation from the general cap of the Main Agreement; exclusions of indirect damages do not apply to administrative fines and notification costs directly caused by a breach attributable to the Processor. Nothing in this DPA limits either Party's liability towards data subjects or overrides Article 82 GDPR.

8.2. The Processor maintains throughout the term of the DPA a professional liability insurance policy covering cyber risks, with **[TO BE COMPLETED: insurer]**, for a minimum amount of **[TO BE COMPLETED: amount]** per claim; a certificate is provided to the Customer at signature and upon request at each renewal.

9. Governing law and jurisdiction

This DPA is governed by **[TO BE CONFIRMED: French]** law, consistent with the Main Agreement (ToS, Section 14). Any dispute relating to its validity, interpretation or performance falls under the exclusive jurisdiction of the courts of **[TO BE CONFIRMED: Paris, France, as under the Main Agreement]**, without prejudice to the mandatory competence of supervisory authorities and of the courts designated by the GDPR.

10. Elected options and signatures

Options elected by the Customer (tick at signature):

- ☐ **"EU-only AI" mode** (Annex 4) — takes effect at signature; includes local/EU transcription of crisis sessions; for the Customer's organisation, AI providers established outside the EU are deemed

removed from the list of authorised sub-processors in Annex 3, and any breach of this configuration constitutes a material breach entitling the Customer to terminate without penalty.

- ☐ **"Critical or important function" (CIF) status** notified as from signature (Annex 5, Part B immediately applicable). Beneficiary financial entity if distinct from the Customer: **[TO BE COMPLETED: legal name, LEI]**

	For the Customer	For the Processor (Cryptaguard BV)
Name	**[TO BE COMPLETED]**	Matthieu Roland
Title	**[TO BE COMPLETED]**	Director
Date		
Signature		

Annex 1 — Description of the processing (Art. 28(3) GDPR)

Subject matter. Provision, as SaaS, of the ResiPlan business continuity and operational resilience platform: business impact analysis (BIA), continuity and recovery plans, risk management, asset and contract inventory (CMDB), regulatory compliance (ISO 22301, DORA, NIS2), exercises and crisis management, with optional AI-assisted features.

Duration. Term of the Main Agreement, plus the return/deletion period provided for in Section 5.8.

Nature of the processing. Hosting, storage, structuring, consultation, modification, export, transmission (notifications), deletion; audio transcription where applicable; AI-assisted content generation where applicable.

Purposes. To enable the Customer to build, operate and demonstrate its business continuity and compliance framework.

Categories of data subjects.

- users of the Service designated by the Customer (employees, executives, contractors);
- members of the Customer's crisis teams and cells, including their alternates;
- professional contacts of third parties entered by the Customer (suppliers, clients, stakeholders, escalation contacts);
- any person mentioned by the Customer in free-text content (incident reports, exercise records, plans, imported documents);
- participants in recorded crisis sessions, where the Customer enables recording (Section 5.10).

Categories of personal data.

- identification and professional contact details: surname, first name, email address, telephone numbers (in particular for crisis directories), function, role, organisation;
- account and usage data: identifiers, login and audit logs (timestamp, IP address, actions);
- free-text business content that may mention individuals: incidents, risks, plans, exercises, comments, imported documents;
- audio recordings and transcripts of crisis sessions, **only where the Customer enables this feature** (Section 5.10).

Special categories of data (Art. 9 GDPR). Regime of Section 6.3: no systematic or structured processing; incidental mentions covered.

Processor's own processing. The processing operations that the Processor carries out as a controller — invoicing and contract management (through its payment provider), commercial relationship management, audience measurement of its website — are described in its privacy policy and fall outside this DPA.

Annex 2 — Technical and organisational measures (Art. 32 GDPR)

The measures below are in force at the date of signature; they may evolve without reducing the overall level of protection (Section 5.3).

Encryption and network

- encryption in transit: TLS 1.2 minimum, TLS 1.3 supported, across all access to the Service; HSTS enabled;
- encryption at rest (AES-256) on the database and file storage; application servers hold no persistent customer data — temporary local-transcription files are deleted once processing completes;
- HTTP security headers (CSP, X-Frame-Options, X-Content-Type-Options) verified in production by automated tests.

Access control and authentication

- password authentication with strength policy, federated login (OAuth) and magic link;
- TOTP two-factor authentication (RFC 6238) with recovery codes: enrolment enforced for platform administration accounts, activation available for every account;
- sessions in secure cookies (`__Host-`, HttpOnly, SameSite), token rotation, remote revocation;
- two-level role-based access control (platform / organisation: administrator, manager, user, viewer), enforced server-side on every function.

Multi-tenant isolation

- every server request is filtered by organisation identifier through dedicated indexes and systematic membership checks;
- any cross-tenant access by a platform administrator is logged and flagged by a persistent warning banner.

Logging and detection

- **cryptographically chained (SHA-256) audit log** covering creations, modifications, deletions, authentication and security events, with before/after states: any tampering is detectable;
- default retention of the application audit log: 7 years (reducible on request, minimum 1 year); high-volume security events are archived to cold storage after 90 days with the integrity chain preserved; technical server access logs are retained for 12 months;
- automated anomaly detection: brute force, credential stuffing, sign-in from an unusual country;
- error and performance monitoring performed **in-house** (no third-party application error-tracking provider).

Application and API security

- rate limiting on endpoints, CSRF protection, input sanitisation (HTML/script neutralisation);
- customer-issued API keys hashed at rest (SHA-256), scoped;
- HMAC signature verification and replay protection (time window) on webhooks;
- production secrets stored outside the codebase, generated with a cryptographic generator.

AI features

- strict input limits and per-organisation isolation of transmitted contexts;

- no use of Customer data for model training, a prohibition imposed contractually on the AI providers as sub-processors (Section 5.4.3);
- per-organisation logging of AI consumption.

Organisation and continuity

- development subject to code review, automated tests (unit, end-to-end, OWASP security tests) and static analysis;
- backups managed by the database infrastructure and snapshot-based deployments allowing rollback; restoration procedure tested at least **[TO BE CONFIRMED: annually]**;
- public vulnerability disclosure procedure compliant with RFC 9116 (`/.well-known/security.txt`);
- least-privilege policy for the Processor's personnel; restricted production access.

Annex 3 — Authorised sub-processors

List in force at the date of signature (Section 5.4; 30 days' prior notice — 60 days in a processing chain — for any change). The up-to-date list is permanently published on the Service's transparency page (`/trust`).

Sub-processor	Purpose	Data concerned	Data location	Transfer safeguards
Convex (Convex, Inc., United States)	Database, serverless functions, real-time sync and file storage	All business and account data of the Service	European Union — AWS eu-west-1 (Ireland), dedicated EU deployment	Data hosted in the EU; US support access covered by SCCs (2021/914)
OVHcloud (OVH SAS, France)	Application hosting (web server of the Service)	Data in transit and technical server logs	European Union — France	No transfer outside the EU
Resend (Resend, Inc., United States)	Transactional email delivery (invitations, notifications, alerts)	Email addresses, content of outgoing emails	United States	SCCs (2021/914)
Anthropic (Anthropic, PBC, United States)	Default AI provider (assistant, plan generation, analyses) — no training on customer data	Contextual content of AI requests (excerpts of organization data needed for the request)	United States	SCCs (2021/914) and, where applicable, an active DPF certification; per-organization "EU-only AI" option available
OpenAI (OpenAI, L.L.C., United States)	Selected AI features and optional cloud transcription of crisis sessions (local alternative available)	Contextual content of AI requests; audio recordings of crisis sessions only when cloud transcription is enabled	United States	SCCs (2021/914) and, where applicable, an active DPF certification; per-organization "EU-only AI" option available
Mistral AI (Mistral AI, France)	"EU-only AI" option: substitute AI provider configurable per organization	Contextual content of AI requests when the organization opts in	European Union — France	No transfer outside the EU
Plausible Analytics (Plausible Insights OÜ, Estonia)	Aggregate, cookieless audience measurement (website and application)	Aggregate traffic statistics (page views, referrer); IP address processed in transit for counting, not stored	European Union	No transfer outside the EU

ICT subcontracting chain (within the meaning of the DORA register of information): rank 1 — the providers in the table above; rank 2 — Amazon Web Services EMEA SARL (hosting infrastructure of the database provider Convex, region eu-west-1, Ireland).

Integrations that the Customer chooses to connect to its own tools (Slack, Microsoft Teams, Discord, SharePoint, outbound webhooks) transmit data to the **Customer's** services: those vendors then act as recipients or processors of the Customer, not of the Processor.

Annex 4 — Transfers outside the European Union

Default location. Service data is hosted in the European Union: database and file storage on the Processor's dedicated European deployment (AWS eu-west-1, Ireland); application servers in France.

Safeguarded transfers. Some sub-processors listed in Annex 3 are established in the United States or may access data from there. For each such transfer, the Processor implements:

- the European Commission's **Standard Contractual Clauses** (Implementing Decision (EU) 2021/914, applicable modules), as the primary safeguard;
- where applicable, the recipient's **active certification under the EU–US Data Privacy Framework (DPF)**, verified at the date of signature;
- for stored data: encryption in transit and at rest;
- for requests sent to AI providers (processed in clear text by nature): **strict minimisation** (only the context necessary for the request is transmitted), a contractual prohibition on training, and zero or strictly limited retention at the provider **[TO BE CONFIRMED: "zero data retention" option subscribed with the AI providers]**;
- a documented transfer risk assessment, provided to the Customer on request.

"EU-only AI" option. Formal election in Section 10. Where elected, the AI features of the Customer's organisation are configured on the European provider listed in Annex 3 (Mistral AI, France) and crisis session transcription is performed locally or in the EU. Four features relying on capabilities specific to the default provider (document compliance analysis, regulatory watch, organisation chart import, assisted mapping) are then unavailable and excluded from the scope of use; the Processor confirms the applied configuration in writing. In this configuration, AI providers established outside the EU are deemed removed from Annex 3 for the Customer's organisation.

Disclosure to third-country authorities. Unless legally prohibited, the Processor notifies the Customer of any binding access request from a third-country authority, challenges it to the reasonable extent possible, and discloses only the minimum required.

Annex 5 — DORA provisions (Art. 30 of Regulation (EU) 2022/2554)

Scope. This annex applies where the Customer is a financial entity within the meaning of DORA or subscribes to the Service on behalf of such an entity. The Service then constitutes an ICT service provided by an ICT third-party service provider; the Customer determines, under its own responsibility, whether the Service **supports a critical or important function** ("CIF") within the meaning of Article 3(22) of DORA, and notifies the Processor in writing (or ticks the election in Section 10). Upon receipt of the notification, the provisions of Part B apply immediately; the Parties formalise the open parameters (the SLA of 30(3)(a), the arrangements of 30(3)(f)) within 30 days. The Customer may notify a change of CIF status at any time, with the same effects. Subcontracting of ICT services supporting a CIF is permitted under the conditions of Section 5.4 and Annex 3, as supplemented by this annex.

Third-party beneficiary. Where the Customer acts on behalf of a financial entity designated in Section 10, that entity — together with its competent and resolution authorities — directly benefits from, and may directly exercise against the Processor, all rights under this annex (access, inspection, on-site audit, TLPT participation, register-of-information data, exit rights), and no amendment of this DPA may reduce those rights without its consent.

Information for the Customer's register of information (Art. 28(3) DORA).

- Provider: Cryptaguard BV — CBE 1007.610.660 — identifier: **[TO BE CONFIRMED: LEI if assigned; failing that, EUID BEKBOBCE1007610660 (BRIS format)]**;
- Type of ICT service (taxonomy of Annex III of Implementing Regulation (EU) 2024/2956): **S19 — Cloud services: SaaS** (business continuity and operational resilience management);
- Location of service provision and of data: European Union (Ireland, France) for application hosting and the database; United States for transactional email delivery and, by default, for AI features ("EU-only AI" option available) — details in Annexes 3 and 4;
- Subcontracting chain with ranks: Annex 3; the Processor provides on request the data in the format of the register-of-information templates (ITS (EU) 2024/2956).

A. Provisions applicable to every arrangement (Art. 30(2))

Ref.	DORA requirement	Contractual implementation
30(2)(a)	Clear and complete description of all functions and ICT services, including subcontracting conditions	Annex 1 of this DPA; Main Agreement; sub-processing regime: Section 5.4 and Annex 3; conditional authorisation of CIF subcontracting: Scope above
30(2)(b)	Locations (regions or countries) of service provision and of data processing/storage, with prior notification of any change	Annexes 3 and 4; 30 days' prior notification of any change of sub-processor **or of location**, including with an unchanged provider (Section 5.4.2)
30(2)(c)	Provisions on availability, authenticity, integrity and confidentiality of data	Annex 2 (encryption, access control, chained audit log ensuring authenticity and integrity, tenant isolation)

Ref.	DORA requirement	Contractual implementation
30(2)(d)	Access, recovery and return of personal and non-personal data in the event of insolvency, resolution, discontinuation of business or termination	Section 5.8: self-service export of all data, personal and non-personal (PDF, Excel/CSV, DOCX, API/JSON), including during the transition period and in the event of insolvency; return in a structured, commonly used and easily accessible format; these commitments survive the opening of any insolvency proceedings affecting the Processor
30(2)(e)	Service level descriptions, including updates and revisions	**[TO BE COMPLETED: reference to the SLA of the Main Agreement or to a dedicated SLA annex — target availability, maintenance windows, support channels and response times]**
30(2)(f)	Assistance in the event of an ICT incident related to the service, at no additional cost or at a cost determined ex ante	The Processor provides assistance related to any ICT incident affecting the Service **at no additional cost** (Sections 5.6 and 5.7)
30(2)(g)	Cooperation with the Customer's competent authorities and resolution authorities, including persons appointed by them	The Processor fully cooperates with the Customer's competent and resolution authorities, and with the persons they appoint, in particular by responding to their requests for information relating to the Service
30(2)(h)	Termination rights and minimum notice periods, in line with the expectations of competent authorities and resolution authorities	Main Agreement **[TO BE COMPLETED: reference]** and Section 5.4.2 (termination without penalty with pro-rata refund); the Customer may additionally terminate in accordance with Article 28 of DORA, in particular in the event of a serious breach, circumstances revealing a deficiency in ICT risk management, or a request from its competent authority
30(2)(i)	Conditions for participation in the Customer's ICT security awareness programmes and digital operational resilience training	Upon the Customer's reasonable request, the Processor's relevant personnel participate remotely in the Customer's awareness actions relating to the use of the Service; the Processor makes its training documentation available

B. Additional provisions where the Service supports a critical or important function (Art. 30(3))

Ref.	DORA requirement	Contractual implementation
30(3)(a)	Full service level descriptions with precise quantitative and qualitative performance targets, kept up to date	**[TO BE COMPLETED: quantified SLA — target monthly availability, RTO/RPO of the Service, support response time objectives, monitoring indicators and revision arrangements]**
30(3)(b)	Provider notice periods and reporting obligations, including notification of any development that could materially impact its ability to provide the service	The Processor notifies the Customer, without undue delay, of any development that could materially affect the Service or its ability to provide it at the agreed levels — including a major incident, change of control, major financial difficulty, loss of a key sub-processor or certification, change of sub-processor or of location (30 days' notice) — via the notification channels of Sections 5.4.2 and 5.6

Ref.	DORA requirement	Contractual implementation
30(3)(c)	Implementation and testing of business contingency plans, and ICT security measures appropriate to the financial entity's regulatory framework	The Processor maintains a continuity and recovery plan for its own operations (backups, snapshot deployments with rollback, restoration procedures) and tests it at least **[TO BE CONFIRMED: annually]**; security measures: Annex 2, maintained at a level appropriate to the regulatory framework applicable to the Customer as notified to the Processor
30(3)(d)	Participation in the Customer's threat-led penetration testing (TLPT) (Art. 26-27 DORA)	The Processor participates and fully cooperates in the Customer's TLPT to the extent the Service falls within the scope of the test, and the absence of prior agreement on practical arrangements shall not delay or condition that participation; reasonable, documented costs are recharged **[TO BE COMPLETED: pricing conditions determined ex ante]**
30(3)(e)	Ongoing monitoring rights: unrestricted access, inspection and audit by the financial entity, any appointed third party and the competent authority; full cooperation during on-site inspections (including by the Lead Overseer); details on scope, procedures and frequency	By way of derogation from the limits in Section 5.9.2 — including the restriction on the choice of auditor — the financial entity (Customer or third-party beneficiary), any third party it appoints and its competent authorities enjoy **unrestricted rights of access, inspection and audit**, including on site, with the right to copy relevant documentation; the Processor fully cooperates during inspections conducted by the entity, its appointees, its competent authorities or the Lead Overseer, commits to providing the requested details on the scope, procedures and frequency of such controls, and no contractual frequency limitation is enforceable
30(3)(f)	Exit strategies: an adequate transition period with continued service and migration assistance, at costs determined ex ante	In the event of termination, the Processor maintains the Service during a transition period of **[TO BE CONFIRMED: 90]** days from the effective date, extendable up to **[TO BE CONFIRMED: 12]** months at the financial entity's request, at pricing conditions determined ex ante **[TO BE COMPLETED: pricing of the transition period and migration assistance]**; it ensures full export of the data in open formats and provides reasonable migration assistance; no default deletion occurs before the end of the transition period (Section 5.8.2); the Customer may test its exit strategy and the Processor shall not object

Document generated from the Service's compliance repository. Fields marked "TO BE COMPLETED" or "TO BE CONFIRMED" must be filled in or confirmed before signature. This document is a draft contract and does not constitute legal advice.