defencelevel

VERSION 1.1 · 1 NOVEMBER 2026

ARTICLE 28 GDPR

# Data Processing Agreement

Between the Customer, as controller, and SCARAFILE Consulting S.R.L., which operates DefenceLevel, as processor.

PREPARED FOR _____

**WHERE THE DATA ARE**
Database and service functions in the European Union (Ireland)

**MY DEFENCE**
Encrypted with AES-256-GCM, with the key outside the database

**INCIDENTS**
Notified to the Customer within 24 hours

**SUB-PROCESSORS**
14 days' written notice before any change

PARTIES

The **Customer**, acting as controller:

| | |
|---|---|
| COMPANY NAME | |
| REGISTERED OFFICE | |
| REGISTRATION NUMBER | |
| VAT NUMBER | |

**SCARAFILE Consulting S.R.L.**, Piața Victoriei 4, ap. 9C, 300006 Timișoara, Romania, trade register J35/2040/2020, VAT RO42858116, which operates the DefenceLevel service (**DefenceLevel**, acting as processor).

PART A

# Terms of this Agreement

## 1 Subject matter and structure

1.1 This Data Processing Agreement (the **Agreement**) applies to the personal data that DefenceLevel processes on behalf of the Customer when it provides the DefenceLevel service under the Terms of Service published at defencelevel.com/terms (the **Main Agreement**), as described in Annex II.

1.2 The Agreement consists of this Part A; Part B, which reproduces the standard contractual clauses between controllers and processors set out in the Annex to Commission Implementing Decision (EU) 2021/915 of 4 June 2021 (the **Clauses**), with the options and the exceptions set out in section 2; and Part C, which contains Annexes I to IV of the Clauses.

1.3 In accordance with Clause 4, the Clauses prevail over this Part A and over the Main Agreement. As regards the processing of personal data, this Part A prevails over the Main Agreement. Part A only adds clauses and safeguards that do not contradict the Clauses.

## 2 Options chosen in the Clauses

2.1 Clause 1(a), Clause 8(c)(4) and Clause 9: Option 1, Regulation (EU) 2016/679 (**GDPR**). Regulation (EU) 2018/1725 does not apply to the parties.

2.2 Clause 5 (docking clause): included.

2.3 Clause 7.7(a): Option 2, general written authorisation, with a notice period of 14 days.

2.4 The Clauses are used in part, as allowed by Article 28(6) GDPR: Clause 2 (invariability) is not used and Clause 7.7(e) is not included (see 5.5). All the other Clauses are reproduced without changes.

## 3 Roles of the parties

3.1 DefenceLevel processes the personal data described in Annex II (**Customer Personal Data**) as processor on behalf of the Customer.

3.2 DefenceLevel processes as an independent controller, under its privacy notice published at defencelevel.com/privacy, the personal data it needs for its own purposes: billing, invoicing, accounting and tax records; payments, which Stripe handles as an independent controller of payment data; the security of the service (connection logs, records of sign-up attempts, anti-bot checks); preventing repeated free trials; visit statistics and measurement of the use of the service; and the establishment, exercise or defence of legal claims. This Agreement does not apply to that processing.

## 4 Instructions

4.1 The Main Agreement, this Agreement and the configuration of the service by the Customer's authorised users (for example their choices in the dashboard and in My Defence) are the Customer's documented instructions under Clause 7.1. The Customer may give further written instructions by email to privacy@defencelevel.com; instructions that change the scope of the service are agreed in writing.

## 5 Sub-processors

5.1 The Customer gives DefenceLevel general written authorisation to engage the sub-processors listed in Annex IV (Clause 7.7(a), Option 2).

5.2 DefenceLevel informs the Customer in writing, by email to the contact person indicated in Annex I, at least 14 days before adding or replacing a sub-processor. The notice states the name and address of the sub-processor, the processing it will carry out, where the data will be processed and, for transfers outside the European Economic Area, the transfer mechanism.

5.3 The Customer may object in writing, with reasons, within those 14 days. The parties then look for a solution in good faith. If no solution is found, either party may terminate the Main Agreement with effect no later than the date on which the change takes effect, without penalty, and DefenceLevel refunds any amount paid for the period after termination. DefenceLevel does not process Customer Personal Data through a sub-processor to which the Customer has objected.

5.4 DefenceLevel forwards to the Customer, within 5 working days of receipt, the notices it receives from the sub-processors in Annex IV about changes to their own sub-processors.

5.5 Clause 7.7(e) of the Commission's clauses requires the processor to agree with each sub-processor a clause in favour of the controller for the case in which the processor disappears, ceases to exist or becomes insolvent. The standard terms of the sub-processors in Annex IV do not provide for such a clause and DefenceLevel cannot negotiate them, so Clause 7.7(e) is not included. To protect the Customer in that case: (a) the Customer's authorised users can delete their accounts and data from the dashboard at any time; (b) My Defence data are encrypted with a key that the database provider does not hold (Annex III); (c) if DefenceLevel decides to stop providing the service, it informs the Customer at least 30 days in advance, returns Customer Personal Data on request and then deletes them, destroying the encryption key as well.

## 6 Personal data breaches and security incidents

6.1 DefenceLevel notifies the Customer of a personal data breach concerning Customer Personal Data without undue delay and in any case within 24 hours of becoming aware of it, by email to the contact person indicated in Annex I. The notification contains the information required by Clause 9.2; information that is not yet available is provided as soon as it is.

6.2 DefenceLevel notifies the Customer in the same way and within the same time of any security incident that compromises, or is reasonably likely to compromise, the confidentiality, integrity or availability of the Customer's data in the service, even when no personal data are involved: for example, unauthorised access to the Customer's My Defence data.

6.3 Within 30 days of the first notification, DefenceLevel sends the Customer a written report on the incident: causes, effects, measures taken and measures planned.

6.4 DefenceLevel does not notify supervisory authorities, CSIRTs or data subjects on behalf of the Customer, unless the Customer instructs it in writing or the law requires it.

## 7 Documentation and audits

7.1 To demonstrate compliance (Clause 7.6(c)), DefenceLevel makes available to the Customer on request: this Agreement with its annexes; a more detailed description of the measures in Annex III, where needed; the summary of the most recent independent security test of the service; and the security reports and certifications that its sub-processors make available to their own customers, insofar as the sub-processors allow them to be shared.

7.2 DefenceLevel answers, free of charge and within 30 days, one security or data protection questionnaire from the Customer every 12 months.

7.3 Where the information under 7.1 and 7.2 is not sufficient, the Customer may carry out an audit itself or through an independent auditor who is bound by confidentiality and is not a competitor of DefenceLevel. The Customer gives at least 30 days' written notice, stating the scope of the audit. Audits take place on working days between 09:00 and 17:00 Romanian time (EET/EEST), do not give access to the data of other customers and do not include the facilities of the sub-processors, which are audited through their own reports. Audits take place at most once every 12 months, unless there are indications of non-compliance, a personal data breach concerning Customer Personal Data or a request from a supervisory authority: in those cases the notice is reasonable for the circumstances.

7.4 Each party bears its own costs of an audit. The Customer bears the costs of its auditor and reimburses DefenceLevel's reasonable costs for the time devoted to the audit beyond one working day, unless the audit reveals a material breach of this Agreement by DefenceLevel.

## 8 Assistance to the Customer

8.1 DefenceLevel forwards to the Customer, within 5 working days, any request from a data subject concerning Customer Personal Data, and does not reply to it itself unless the Customer authorises it (Clause 8(a)).

8.2 The Customer's authorised users can change their preferences and their My Defence data, and delete their account, themselves in the dashboard. On request of the Customer, DefenceLevel exports Customer Personal Data in a structured, machine-readable format (JSON) within 30 days.

8.3 For data protection impact assessments and prior consultations, DefenceLevel provides the information in this Agreement and, on request, reasonable further information about the service.

## 9 End of the processing

9.1 When the Main Agreement ends, the Customer chooses by written notice between deletion and return of Customer Personal Data (Clause 10(d)). If the Customer has not chosen within 30 days, DefenceLevel asks it in writing; if no choice is made within a further 30 days, DefenceLevel deletes the data.

9.2 DefenceLevel deletes Customer Personal Data from the service's database within 30 days of the Customer's choice. Copies in the database backups expire within 7 days of the deletion; the data of sent emails held by the email sub-processor expire within 30 days. DefenceLevel certifies the deletion in writing on request.

9.3 If the Customer chooses return, DefenceLevel exports Customer Personal Data in a structured, machine-readable format (JSON) within 30 days and then deletes it as described in 9.2.

9.4 Personal data that DefenceLevel must keep by law, such as invoices, are processed as an independent controller under 3.2.

## 10 Liability

10.1 The liability of each party under this Agreement is governed by the Main Agreement. Nothing in this Agreement limits the rights of data subjects under Article 82 GDPR.

## 11 Term and changes

11.1 This Agreement applies from its signature for as long as DefenceLevel processes Customer Personal Data under the Main Agreement, and afterwards until the data are deleted or returned.

11.2 Changes to this Agreement require the written agreement of both parties, except: updates to Annex IV made under section 5; and updates to Annexes II and III that DefenceLevel notifies in writing at least 14 days in advance and that do not reduce the level of protection of Customer Personal Data.

## 12 Governing law and jurisdiction

12.1 This Agreement is governed by Romanian law. The courts of Timișoara, Romania, have exclusive jurisdiction, as in the Main Agreement. This does not affect the rights of data subjects or the powers of supervisory authorities under the GDPR.

## 13 Signature

13.1 The parties sign this Agreement, including Annex I, in writing, also in electronic form.

| FOR THE CUSTOMER | FOR SCARAFILE CONSULTING S.R.L. |
|---|---|
| NAME | NAME |
| | Alessandro Scarafile |
| POSITION | POSITION |
| | Administrator |
| DATE | DATE |
| SIGNATURE | SIGNATURE |

PART B

# Standard contractual clauses

> Text of the Annex to Commission Implementing Decision (EU) 2021/915 of 4 June 2021 (OJ L 199, 7.6.2021, p. 18), as published on EUR-Lex, with the options and the two exceptions set out in Part A, section 2. Nothing else is changed.

SECTION I

## CLAUSE 1 Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

## CLAUSE 2 Invariability of the Clauses

Not used: the Clauses are used in part (Part A, 2.4).

## CLAUSE 3 Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

## CLAUSE 4 Hierarchy

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

### CLAUSE 5 · OPTIONAL Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

## SECTION II OBLIGATIONS OF THE PARTIES

### CLAUSE 6 Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

### CLAUSE 7 Obligations of the Parties

#### 7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

#### 7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

#### 7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

#### 7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 7.5. Sensitive data

If the processing 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 ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

### 7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

### 7.7. Use of sub-processors

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) Not included (Part A, 2.4 and 5.5).

### 7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

## CLAUSE 8 Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

> (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
>
> (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
>
> (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
>
> (4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

## CLAUSE 9 Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

### 9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

### 9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

## SECTION III FINAL PROVISIONS

### CLAUSE 10 Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

PART C

# Annexes to the Clauses

ANNEX I

## List of parties

CONTROLLER(S)

| | |
|---|---|
| NAME | |
| ADDRESS | |
| CONTACT PERSON'S NAME, POSITION AND CONTACT DETAILS | |
| DATA PROTECTION OFFICER, WHERE APPLICABLE | |
| SIGNATURE AND ACCESSION DATE | |

PROCESSOR(S)

| | |
|---|---|
| NAME | SCARAFILE Consulting S.R.L. (DefenceLevel) |
| ADDRESS | Piața Victoriei 4, ap. 9C, 300006 Timișoara, Romania |
| CONTACT PERSON'S NAME, POSITION AND CONTACT DETAILS | Alessandro Scarafile, Administrator, privacy@defencelevel.com; security incidents and vulnerability reports: security@defencelevel.com |
| DATA PROTECTION OFFICER | not appointed (not required under Article 37 GDPR) |
| SIGNATURE AND ACCESSION DATE | |

ANNEX II

# Description of the processing

### CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED

Authorised users of the Customer: employees, contractors and other persons to whom the Customer gives access to the DefenceLevel service, each with their own account linked to an email address.

Persons named by an authorised user to receive a copy of the DEFCON 1 and 2 alerts (for example a colleague or a team mailbox), who have no account: only their email address, which receives copies after they confirm it.

### CATEGORIES OF PERSONAL DATA PROCESSED

1. Account data: email address, preferred language, status of the account and of the subscription bought by the Customer, sign-in and session data (single-use sign-in links, session identifiers; for each sign-in of the last 90 days: date and time, browser, operating system, type of device and country, without the IP address).
2. Service preferences: choices about the briefing and the alerts by email, pause of the emails; the second address for the alerts, if a user enters one, with the status of its confirmation.
3. My Defence data: the zones of the infrastructure diagram, with their names, descriptions and connections; the vendors and products chosen; the free-text notes on the zones. These data describe the Customer's systems and are not normally personal data: they become personal data only if a user writes personal data in names, descriptions or notes, which the Customer should avoid.
4. Records of the emails sent: which service emails were sent to each user, when, their delivery status and, for the briefing and the alerts, the My Defence choice at the time of sending.
5. Correspondence: the messages that users send to DefenceLevel's addresses about the service.

### SENSITIVE DATA PROCESSED (IF APPLICABLE) AND APPLIED RESTRICTIONS OR SAFEGUARDS

None. The service does not need special categories of personal data or data relating to criminal convictions and offences, and the Customer does not enter them in the free-text fields.

### NATURE OF THE PROCESSING

Collection from the Customer's authorised users; storage in a managed database, with application-level encryption of My Defence data; comparison of the products chosen with public vulnerability data; generation and sending of the emails of the service (daily briefing, alerts); display in the dashboard; export and deletion.

### PURPOSE(S) FOR WHICH THE PERSONAL DATA IS PROCESSED ON BEHALF OF THE CONTROLLER

Providing the DefenceLevel service to the Customer: the daily briefing, the alerts, the dashboard and, with My Defence, the selection of the briefing items and of the alerts that concern the Customer's products.

### DURATION OF THE PROCESSING

For the term of the Main Agreement and until the deletion or return of the data under Clause 10(d) and section 9 of Part A.

### FOR PROCESSING BY (SUB-) PROCESSORS, ALSO SPECIFY SUBJECT MATTER, NATURE AND DURATION OF THE PROCESSING

As described for each sub-processor in Annex IV, for the same duration.

ANNEX III

# Technical and organisational measures

> The measures are described as they are in place at the date of this Agreement.

### ENCRYPTION AND PSEUDONYMISATION

- In transit: the service is reachable only over HTTPS, with HTTP Strict Transport Security (two years, subdomains included). Connections between the service functions and the database are encrypted.
- At rest: the database provider encrypts the disks and the backups (AES-256).
- Application-level encryption of My Defence data: vendors, products, diagram and zone notes are encrypted with AES-256-GCM before being written to the database. The keys are derived (HKDF-SHA-256) from a master key that is not stored in the database: it is kept in the encrypted environment settings of the hosting provider and in the administrator's password manager. Each encrypted text is bound to its account, so that it cannot be decrypted if copied to another account. Choices already made are recognised through HMAC-SHA-256 fingerprints that differ from one account to another. The data are decrypted only in memory, to show them to the user and to select the briefing items and the alerts.

### CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

- Database: row-level security enabled on every table; no access granted to the roles of the provider's public interfaces; the provider's data API exposes only an empty schema; the service connects with its own credentials.
- Artificial intelligence: the AI checks that write and verify the texts of the briefing and of the alerts read only public vulnerability data, through a dedicated read-only database user that cannot read the tables with the data of users, accounts or My Defence.
- Maintenance: the administrator reads the production database in read-only transactions; changes are made only with scripts reviewed for the purpose.
- Sign-in and sign-up are protected by per-IP-address rate limits on the hosting provider's firewall and by an anti-bot check.
- Security headers on every page: Content Security Policy, X-Frame-Options DENY, X-Content-Type-Options nosniff, a strict Referrer-Policy and a Permissions-Policy.
- Serverless functions and managed database run by the sub-processors in Annex IV; uptime of the scheduled jobs monitored by an external service with alerts to the administrator.

### ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER

- Daily database backups, encrypted, kept for 7 days by the database provider.
- Code and configuration in a private version-controlled repository, from which the service can be deployed again.

### REGULAR TESTING, ASSESSMENT AND EVALUATION OF THE EFFECTIVENESS OF THE MEASURES

- An automated test suite (more than 760 tests) runs before every deployment, together with a dry run that compares the output of the new version with the current one; every deployment is approved by the administrator.
- An independent penetration test of the web application and of its interfaces, with authenticated access, is planned for November 2026, then at least once a year and after significant changes. Its summary is available to the Customer on request.

- Vulnerability disclosure: published policy (defencelevel.com/security and security.txt), acknowledgment of reports within 5 working days.

### USER IDENTIFICATION AND AUTHORISATION

- Sign-in without passwords, through signed links that can be used once and are valid for 30 minutes.
- Sessions in HttpOnly, Secure, SameSite=Lax cookies, valid for at most 30 days and removed at sign-out.
- Each user sees the latest sign-ins to their account on the Account page of the dashboard and can sign out all other devices: the other sessions and the sign-in links not used yet stop working at once.
- Each account sees only its own data: every request is checked against the signed-in account.
- The administration area is reserved to the administrator's account and shows only how many products and zones an account has, never which ones, nor the notes.
- The administrator's accounts at all the providers of the service are protected by two-factor authentication, directly or through sign-in with a Google or GitHub account protected by two-factor authentication.

### PROTECTION OF DATA DURING TRANSMISSION AND STORAGE

As described under Encryption and pseudonymisation.

### PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED

- Personal data are processed in the data centres of the sub-processors listed in Annex IV, under their physical security measures and certifications.
- The administrator's computer has full-disk encryption.

### EVENTS LOGGING

- Request logs of the hosting provider, kept for the period set by the provider; records of the emails sent and of the use of sign-in links in the service's database; logs of the database provider.

### SYSTEM CONFIGURATION, INCLUDING DEFAULT CONFIGURATION

- My Defence is optional and empty by default; without it the service works with all its emails.
- No advertising or profiling cookies; visit statistics without cookies and without storing IP addresses.

### INTERNAL IT AND IT SECURITY GOVERNANCE AND MANAGEMENT

- The service is run by its administrator, who is the only person with access to production systems and data and is bound by confidentiality.
- Secrets are kept in the hosting provider's encrypted environment settings and in a password manager, never in the code repository.
- Written internal rules for deployments (tests, dry run, explicit approval) and for access to the production database (read-only by default).

### CERTIFICATION AND ASSURANCE OF PROCESSES AND PRODUCTS

- DefenceLevel holds no certification of its own. The sub-processors in Annex IV hold independent certifications or audit reports, such as SOC 2 Type 2 or ISO/IEC 27001, described in their security documentation.

### DATA MINIMISATION, DATA QUALITY AND LIMITED RETENTION

- Only the email address is required to use the service; no names, telephone numbers or payment card data are needed (payments are handled by Stripe as an independent controller).
- Users can correct their data and choices in the dashboard at any time.

- Data are deleted when the account is deleted; copies in the database backups expire within 7 days; the data of sent emails held by the email sub-processor expire within 30 days; sign-in records are deleted after 90 days.

### ACCOUNTABILITY

- This Agreement, the privacy notice and the page on the protection of My Defence data (defencelevel.com/data-protection) describe the processing; changes to the service and to the measures are recorded in the code repository.

### DATA PORTABILITY AND ERASURE

- Export of Customer Personal Data in a structured, machine-readable format (JSON) from the Account page of the dashboard or on request; erasure through account deletion in the dashboard or on request.

### MEASURES TO ASSIST THE CONTROLLER (CLAUSES 8 AND 9)

- Requests from data subjects forwarded to the Customer within 5 working days (Part A, 8.1).
- Personal data breaches and security incidents notified within 24 hours, by email to the contact person in Annex I, followed by a written report within 30 days (Part A, section 6). Each notification includes, besides the elements of Clause 9.2: the time at which the breach occurred and the time at which DefenceLevel became aware of it, in UTC; the data and accounts concerned; whether the data concerned were encrypted at application level.
- Information for data protection impact assessments and prior consultations on request (Part A, 8.3).
- Contacts: privacy@defencelevel.com; security@defencelevel.com.

### MEASURES OF THE SUB-PROCESSORS

The sub-processors apply the technical and organisational measures described in their data processing agreements and security documentation, which impose on them, in substance, the obligations of the Clauses (Clause 7.7(b)).

ANNEX IV

# List of sub-processors

> Agreed list under Clause 7.7(a), Option 2, at the date of this Agreement.

### Vercel Inc.

| | |
|---|---|
| ADDRESS | 440 N Barranca Ave #4133, Covina, CA 91723, United States |
| CONTACT | privacy@vercel.com |
| DESCRIPTION OF THE PROCESSING | hosting of the website and of the service's serverless functions, which run in the European Union (region dub1, Dublin, Ireland); content delivery network. Processes Customer Personal Data while the service runs, and request logs. |
| TRANSFERS | the company is in the United States; EU–US Data Privacy Framework (active certification) and standard contractual clauses (Decision (EU) 2021/914) in Vercel's data processing agreement. |

### Supabase Pte. Ltd.

| | |
|---|---|
| ADDRESS | 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513 |
| CONTACT | security@supabase.com and the privacy contacts in Supabase's data processing agreement |
| DESCRIPTION OF THE PROCESSING | managed PostgreSQL database in the European Union (region eu-west-1, Ireland): storage of all Customer Personal Data, with My Defence data encrypted at application level by DefenceLevel; daily backups kept for 7 days. |
| TRANSFERS | the company is in Singapore, which has no adequacy decision: standard contractual clauses (Decision (EU) 2021/914) in Supabase's data processing agreement; the database stays in the European Union. |

### Plus Five Five, Inc. (Resend)

| | |
|---|---|
| ADDRESS | 2261 Market Street #5039, San Francisco, CA 94114, United States |
| CONTACT | privacy@resend.com |
| DESCRIPTION OF THE PROCESSING | sending of the service's emails from the European Union (region eu-west-1, Ireland): recipients' email addresses and email content. Account data, email metadata and logs are stored in the United States; the data of sent emails are kept for 30 days. |
| TRANSFERS | EU–US Data Privacy Framework (active certification) and standard contractual clauses (Decision (EU) 2021/914) in Resend's data processing agreement. |

**OVH Hosting Limited (OVHcloud)**

| | |
|---|---|
| ADDRESS | Block 3, Harcourt Centre, Harcourt Road, D02 A339 Dublin 2, Ireland (registration number 468585) |
| CONTACT | the data protection contact in OVHcloud's data processing agreement |
| DESCRIPTION OF THE PROCESSING | mailbox of the @defencelevel.com addresses, which receives the messages that users send to DefenceLevel. Data hosted in France. |
| TRANSFERS | none outside the European Economic Area; group companies in Canada and the United Kingdom, countries with an adequacy decision, may access the data for maintenance. |

**Not sub-processors.** Stripe processes payment data as an independent controller. Product names that the catalogue of the service does not know are looked up in NIST's National Vulnerability Database without any data about the Customer or its users. The AI service that writes and checks the texts of the briefing (Anthropic) receives only public vulnerability data, never Customer Personal Data. The monitoring service of the scheduled jobs (Healthchecks.io) receives no personal data.