
DATA PROCESSING AGREEMENT/ADDENDUM

This Data Processing Agreement (“**DPA**”) supplements any current Cynet Terms and Conditions, Partner Agreement or other similar agreement (each “**Agreement**”) made between **Cynet** as defined below (“**Cynet**”, “**Us**”, “**We**”, “**Our**”, or “**Data Processor**”) and the Client (defined below) (collectively, “**You**”, “**Your**”, “**Client**”, or “**Data Controller**”). You acknowledge that you have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with Cynet to reflect the parties’ agreement with regard to the Processing of Personal Data (as such terms are defined below) of GDPR-protected individuals. Both parties shall be referred to as the “**Parties**” and each, a “**Party**”.

WHEREAS, Cynet shall provide the services set forth in the Agreement (collectively, the “**Services**”) for Client, as described in the Agreement; and

WHEREAS, In the course of providing the Services pursuant to the Agreement, we may process Personal Data on your behalf, in the capacity of a “**Data Processor**”; and the Parties wish to set forth the arrangements concerning the processing of Personal Data (defined below) within the context of the Services and agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

NOW THEREFORE, in consideration of the mutual promises set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by the Parties, the parties, intending to be legally bound, agree as follows:

1. INTERPRETATION AND DEFINITIONS

- 1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA.
- 1.2 References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.
- 1.3 Words used in the singular include the plural and vice versa, as the context may require.
- 1.4 Capitalized terms not defined herein shall have the meanings assigned to such terms in the Agreement.
- 1.5 Definitions:
 - (a) “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “**Control**”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
 - (b) “**Authorized Affiliate**” means any of Client’s Affiliate(s) which (a) is subject to the Data Protection Laws And Regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Client and Cynet, but has not signed its own agreement with Cynet and is not a “**Client**” as defined under the Agreement.
 - (c) “**Controller**” or “**Data Controller**” means the entity which determines the purposes and means of the Processing of Personal Data, as specified under the GDPR and other relevant Data Protection Laws and Regulations. For the purposes of this DPA only, and except where indicated otherwise, the term “Data Controller” shall include yourself, the Organization and/or the Organization’s Authorized Affiliates.
 - (d) “**Cynet**” means the relevant Cynet entity of the following Cynet legal entities: Cynet Security Ltd., Cynet Security, Inc., Cynet Security Italy SRL and Cynet Security UK LTD.
 - (e) “**Cynet Group**” means Cynet and its Affiliates engaged in the Processing of Personal Data.
 - (f) “**Client**” means (i) the person or entity that is indicated below in the signature block, or (ii) if there is no signature block or it is not completed, then Client is the person or entity that has entered into the Agreement with Client. Client also means a Client Affiliate when: (i) Data Protection Laws and Regulations require a direct relationship between Cynet and the Client’s Affiliate with respect to data protection agreements, (ii) Client is duly and effectively authorized (or subsequently ratified) to act on its Affiliate’s behalf, and (iii) Cynet processes the Affiliate’s Client Personal Data;
 - (g) “**Data Protection Laws and Regulations**” means (a) European Union or Member State laws, including GDPR, with respect to Organization’s Personal Data which is subjected to EU Data Protection Laws; (b) the California Consumer Privacy Act of 2018 (“**CCPA**”) with respect to any of Organization’s Personal Data in respect of which Organization’s is subject to the CCPA, and (c) any other applicable law with respect to any of Organization’s Personal Data in respect of which Organization is subject to any other Data Protection Laws.
 - (h) “**Data Subject**” means the identified or identifiable person to whom the Personal Data relates.

- (i) **“DPA Effective Date”**
- (j) **“Member State”** means a country that belongs to the European Union and/or the European Economic Area. **“Union”** means the European Union.
- (k) **“GDPR”** means the 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).
- (l) **“Personal Data”** means any information relating to an identified or identifiable natural person; 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.
- (m) **“Process(ing)”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.
- (n) **“Processor”** or **“Data Processor”** means the entity which Processes Personal Data on behalf of the Controller.
- (o) **“Standard Contractual Clauses”** or **“SCCs”** means (i) the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out in Regulation (EU) 2016/679 of the European Parliament and of the Council from June 4, 2021, as available [here](#), as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a supervisory authority for use with respect to any specific restricted transfer, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by Applicable Laws for use in respect of such Restricted Transfer, as updated, amended, replaced or superseded from time to time by such Regulatory Authority or Data Protection Laws and Regulations;
- (p) **“Sub-processor”** means any Processor engaged by Cynet and/or Cynet.
- (q) **“Supervisory Authority”** means an independent public authority which is established by an EU Member State pursuant to the GDPR.
- (r) **“UK GDPR”** means the Data Protection Act 2018, as updated, amended, replaced or superseded from time to time by the ICO.
- (s) **“UK Standard Contractual Clauses”** or **“UK SCCs”** means the standard contractual clauses for the transfer of Personal Data to Data processors established in third countries which do not ensure an adequate level of protection as set out by the ICO, as available [here](#), as updated, amended, replaced or superseded from time to time by the ICO.

2. PROCESSING OF PERSONAL DATA

- 2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data, (i) Client shall be considered in the context of the GDPR the Data Controller, and in the context of the CCPA as the business (ii) Cynet shall be considered in the context of the GDPR as the Data Processor, and in the context of the CCPA as the service provider and that (iii) Cynet or members of the Cynet Group may engage Sub-processors pursuant to the requirements set forth in Section 5 “Authorization Regarding Sub-processors” below.
- 2.2 **Client’s Processing of Personal Data.** Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations and comply at all times with the obligations applicable to data controllers (including, without limitation, Article 24 of the GDPR). For the avoidance of doubt, Client’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the means by which Client acquired Personal Data. Without limitation, Client shall comply with any and all transparency-related obligations (including, without limitation, displaying any and all relevant and required privacy notices or policies) and shall have any and all required legal bases in order to collect, Process and transfer to Cynet the Personal Data and to authorize the Processing by Cynet of the Personal Data which is authorized in this DPA. Client shall ensure that any disclosure or transfer of Personal Data to Cynet complies with the Data Protection Laws and Regulations, and inform Cynet about any erroneous, rectified, updated or deleted personal data subject to the Cynet’s processing. Client shall fully comply with any request of data subjects and with any data subject rights under Data Protection Laws and Regulations. Client shall ensure that only such employees that are handling consumer inquiries about the business’s privacy practices or the business’s compliance with the CCPA, have received appropriate training and instructions regarding the CCPA and especially sections 1798.100, 1798.105, 1798.110, 1798.115 and 1798.125 of the CCPA, and how to direct consumers to exercise their rights under such sections. Client shall defend, hold harmless and indemnify Cynet, its Affiliates and subsidiaries (including without limitation their directors, officers, agents, subcontractors and/or employees) from and against any liability of any kind related to any breach, violation or infringement by Client and/or its authorized users of any Data Protection Laws and Regulations and/or this DPA and/or this Section.

2.3 Cynet's Processing of Personal Data.

- 2.3.1 Subject to the Agreement, Cynet shall Process Personal Data only in accordance with Client's documented instructions as necessary for the performance of the Services and for the performance of the Agreement and this DPA, unless required to otherwise by Union or Member State law to which Cynet is subject, in which case, Cynet shall inform the Client of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The duration of the Processing, the nature and purposes of the Processing, as well as the types of Personal Data Processed and categories of Data Subjects under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.
- 2.3.2 To the extent that Cynet cannot comply with a request (including, without limitation, any instruction, direction, code of conduct, certification, or change of any kind) from Client and/or its authorized users relating to Processing of Personal Data or where Cynet considers such a request to be unlawful, Cynet (i) shall inform Client, providing relevant details of the problem, (ii) Cynet may, without any kind of liability towards Client, temporarily cease all Processing of the affected Personal Data (other than securely storing those data), and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, each Party may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Client shall pay to Cynet all the amounts owed to Cynet or due before the date of termination. Client will have no further claims against Cynet (including, without limitation, requesting refunds for Services) due to the termination of the Agreement and/or the DPA in the situation described in this paragraph (excluding the obligations relating to the termination of this DPA set forth below).
- 2.3.3 Cynet will not be liable in the event of any claim brought by a third party, including, without limitation, a Data Subject, arising from any act or omission of Cynet, to the extent that such is a result of Client's instructions.
- 2.3.4 If Client provides Cynet or any of the entities of the Cynet Group with instructions, requests, suggestions, comments or feedback (whether orally or in writing) with respect to the Services, Client acknowledges that any and all rights, including intellectual property rights, therein shall belong exclusively to Cynet and that such shall be considered Cynet's intellectual property without restrictions or limitations of any kind, and Client hereby irrevocably and fully transfers and assigns to Cynet any and all intellectual property rights therein and waives any and all moral rights that Client may have in respect thereto.

3. **RIGHTS OF DATA SUBJECTS**

If Cynet receives a request from a Data Subject to exercise its right to be informed, right of access, right to rectification, erasure, restriction of Processing, data portability, right to object, or its right not to be subject to a decision solely based on automated processing, including profiling ("**Data Subject Request**"), Cynet shall, to the extent legally permitted, notify and forward such Data Subject Request to Client, and the Client shall act in accordance with the relevant provisions imposed on it for the purpose of exercising the rights of the data subject under the Data Protection Laws and Regulations. Taking into account the nature of the Processing, Cynet shall assist Client by appropriate technical and organizational measures, insofar as this is possible from Cynet's point of view, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from Cynet's provision of such assistance.

4. **CYNET PERSONNEL**

- 4.1 Confidentiality. Cynet shall grant access to the Personal Data to its personnel's, agents and/or contractors only on a need to know basis and shall take reasonable measures to ensure that they who may have access to the Processing of Personal Data, have committed themselves to confidentiality and non-disclosure.
- 4.2 Cynet may disclose and Process the Personal Data (a) as permitted hereunder (b) to the extent required by a court of competent jurisdiction or other Supervisory Authority and/or otherwise as required by applicable laws or applicable Data Protection Laws and Regulations (in such a case, Cynet shall inform the Client of the legal requirement before the disclosure, unless that law prohibits such information on important grounds of public interest), or (c) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

5. **AUTHORIZATION REGARDING SUB-PROCESSORS**

- 5.1.1 Cynet's current list of Sub-processors it is hereby approved by Data Controller as **Schedule 2**. Such Sub-processor list shall include the identities and details of those Sub-processors and their country of location ("**Sub-processor List**"). The Sub-processor List as of the date of execution of this DPA, or as of the date of publication (as applicable), is hereby, or shall be (as applicable), authorized by Client.
- 5.1.2 Client shall send an email to privacy@cynet.com to subscribe to notifications of new Sub-processors, and if Client subscribes, Cynet shall provide notification of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Services.
- 5.1.3 Objection Right for New Sub-processors. In any event, the Sub-processor List as specified in **Schedule 2** shall be

deemed authorized by Client. Without derogating from the above, Client may reasonably object to Cynet's use of a new Sub-processor for reasons related to the GDPR by notifying Cynet promptly in writing within three (3) business days after receipt of Cynet's notice in accordance with the mechanism set out in Section 5.1.2. and such written objection shall include the reasons related to the GDPR for objecting to Cynet's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within three (3) business days following Cynet's notice shall be deemed as acceptance of the new Sub-Processor. In the event Client reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Cynet will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Client. If Cynet is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, either party may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those Services which cannot be provided by Cynet without the use of the objected-to new Sub-processor by providing written notice to the other party, provided that all amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Cynet by the Client. Until a decision is made regarding the new Sub-processor, Cynet may temporarily suspend the Processing of the affected Personal Data. Client will have no further claims against Cynet due to the termination of the Agreement (including, without limitation, requesting refunds) and/or the DPA in the situation described in this paragraph.

- 5.1.4 Agreements with Sub-processors. Cynet shall respect the Data Protection Laws and Regulations when engaging another processor for Processing Personal Data provided by Client.

6. SECURITY

- 6.1 Controls for the Protection of Personal Data. Taking into account the state of the art, Cynet shall maintain all industry-standard technical and organizational measures required pursuant to Article 32 of the GDPR for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data, as set forth in the Security Documentation which are hereby approved by Client. At the minimum, Cynet will use the technical and organizational measures specified in Schedule 3. Upon the Client's request, Cynet will use commercially reasonable efforts to assist Client, at Client's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing, the state of the art, and the information available to Cynet.
- 6.2 Third-Party Certifications and Audits. Upon Client's written request of at least thirty (30) days to Cynet and not more than once per calendar year, and subject to the confidentiality obligations set forth in the Agreement and this DPA, Cynet shall make available to Client that is not a competitor of Cynet (or Client's independent, third-party auditor that is not a competitor of Cynet) a copy of Cynet's then most recent third-party audits or certifications, as applicable (provided, however, that such audits, certifications and the results therefrom, including the documents reflecting the outcome of the audit and/or the certifications, shall only be used by Client to assess compliance with this DPA and/or with applicable Data Protection Laws and Regulations, and shall not be used for any other purpose or disclosed to any third party without Cynet's prior written approval and, upon Cynet's first request, Client shall return all records or documentation in Client's possession or control provided by Cynet in the context of the audit and/or the certification). At Client's cost and expense, Cynet shall allow for and contribute to audits, including inspections of physical premises, conducted by the controller or another auditor mandated by the controller (who is not a direct or indirect competitor of Cynet) provided that the parties shall agree in advance and in good faith on the scope, methodology, timing and conditions of such audits and inspections. It is clarified that such audit and inspection procedures shall be conducted not more than once per calendar year and with prior written notice to Cynet of at least thirty (30) days. It is further clarified that the Client and/or authorized auditor on its behalf under this section, shall ensure that no interruption is made to the Organization's routine operations, and that such proceedings shall be conducted during Cynet's business hours.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

Cynet maintains security incident management policies and procedures specified in Security Documentation and, to the extent required under applicable Data Protection Laws and Regulations, shall notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including Personal Data transmitted, stored or otherwise Processed by Cynet or its Sub-processors of which Cynet becomes aware (a "**Personal Data Incident**"). Cynet shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as Cynet deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within Cynet's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's users. In any event, Client will be the party responsible for notifying supervisory authorities and/or concerned data subjects (where required by Data Protection Laws and Regulations).

8. RETURN AND DELETION OF PERSONAL DATA

Subject to the Agreement, Cynet shall, at the choice of Client, delete or return the Personal Data to Client after the end of the provision of the Services relating to processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. In any event, to the extent required or allowed by applicable law, Cynet may retain one copy of the Personal Data

for evidence purposes and/or for the establishment, exercise or defence of legal claims and/or to comply with applicable laws and regulations. If the Client requests the Personal Data to be returned, the Personal Data shall be returned in the format generally available for Cynet's Clients.

9. AUTHORIZED AFFILIATES

- 9.1 Contractual Relationship. The Parties acknowledge and agree that, by executing the DPA, the Client enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Cynet. Each Authorized Affiliate agrees to be bound by the obligations under this DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Client.
- 9.2 Communication. The Client shall remain responsible for coordinating all communication with Cynet under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10. TRANSFERS OF DATA

- 10.1 Transfers to countries that offer adequate level of data protection. Personal Data may be transferred from the EU Member States, the three EEA member countries (Norway, Liechtenstein and Iceland) and the United Kingdom (collectively, "EEA") to countries that offer adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the Union, the Member States or the European Commission ("Adequacy Decisions"), without any further safeguard being necessary.
- 10.2 Transfers to other countries. If the Processing of Personal Data includes transfers from the EEA to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision ("Other Countries"), the Parties shall comply with the below terms:
- a) With respect to the EU transfers of Personal Data, Client as a Data Exporter (as defined in the SCCs) and Cynet on behalf of itself and each Cynet Affiliate (as applicable) as a Data Importer (as defined in the SCCs) hereby enter into the Standard Contractual Clauses set out in **Schedule 4**. To the extent that there is any conflict or inconsistency between the terms of the Standard Contractual Clauses and the terms of this DPA, the terms of the Standard Contractual Clauses shall take precedence.
 - b) With respect to the UK transfers of Personal Data (from the UK to other countries which have not been subject to a relevant Adequacy Decision), Client as a Data Exporter (as defined in the SCCs) and Cynet on behalf of itself and each Cynet Affiliate (as applicable) as a Data Importer (as defined in the SCCs), hereby enter into the UK Standard Contractual Clauses set out in **Schedule 4**.

11. TERMINATION

This DPA shall automatically terminate upon the termination or expiration of the Agreement under which the Services are provided. Sections 2.2, 2.3.3, 2.3.4 and 12 shall survive the termination or expiration of this DPA for any reason. This DPA cannot, in principle, be terminated separately to the Agreement, except where the Processing ends before the termination of the Agreement, in which case, this DPA shall automatically terminate.

12. RELATIONSHIP WITH 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.

Notwithstanding anything to the contrary in the Agreement and/or in any agreement between the parties and to the maximum extent permitted by law: (A) Cynet's (including Cynets' Affiliates') entire, total and aggregate liability, related to, or for breach of, this DPA and/or Data Protection Laws and Regulations, including, without limitation, if any, any indemnification obligation under the Agreement or applicable law regarding data protection or privacy, shall be limited to the amounts paid to Cynet under the Agreement within twelve (12) months preceding the event that gave rise to the claim. This limitation of liability is cumulative and not per incident; (B) In no event will Cynet and/or Cynet Affiliates and/or their third-party providers, be liable under, or otherwise in connection with this DPA for: (i) any indirect, exemplary, special, consequential, incidental or punitive damages; (ii) any loss of profits, business, or anticipated savings; (iii) any loss of, or damage to data, reputation, revenue or goodwill; and/or (iv) the cost of procuring any substitute goods or services; and (C) The foregoing exclusions and limitations on liability set forth in this Section shall apply: (i) even if Cynet, Cynet Affiliates or third-party providers, have been advised, or should have been aware, of the possibility of losses or damages; (ii) even if any remedy in this DPA fails of its essential purpose; and (iii) regardless of the form, theory or basis of liability (such as, but not limited to, breach of contract or tort).

13. AMENDMENTS

This DPA may be amended at any time by a written instrument duly signed by each of the Parties.

14. LEGAL EFFECT

This DPA shall only become legally binding between Client and Cynet when the formalities steps set out in the Section "INSTRUCTIONS ON HOW TO EXECUTE THIS DPA" below have been fully completed.

15. SIGNATURE

The Parties represent and warrant that they each have the power to enter into, execute, perform and be bound by this DPA.

You, as the signing person on behalf of Client, represent and warrant that you have, or you were granted, full authority to bind the Organization and, as applicable, its Authorized Affiliates to this DPA. If you cannot, or do not have authority to, bind the Organization and/or its Authorized Affiliates, you shall not supply or provide Personal Data to Cynet.

By signing this DPA, Client enters into this DPA on behalf of itself and, to the extent required or permitted under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent that Cynet processes Personal Data for which such Authorized Affiliates qualify as the/a "data controller".

The Parties by their duly authorized representatives have executed this DPA to be effective as of the DPA Effective Date.

Cynet

Signed by:

Nir Donitza

FA69898C2CE848D...

Signature

Nir Donitza

Printed Name

CFO

Title

March 4, 2026

Date

Send notices to: legal@cynet.com

Client: _____

Signature

Printed Name

Title

Date

Notice Address: _____

List of Schedules

- **SCHEDULE 1 - DETAILS OF THE PROCESSING**
- **SCHEDULE 2 - SUB-PROCESSOR LIST**
- **SCHEDULE 3 - TECHNICAL AND ORGANIZATIONAL MEASURES**
- **SCHEDULE 4 – STANDARD CONTRACTUAL CLAUSES**

INSTRUCTIONS FOR CREATING A LEGALLY BINDING DPA:

This DPA been pre-signed on behalf of Cynet.

This DPA will become legally binding when Client:

1. Completes the information in the signature box of this DPA;
2. Signs the DPA in the signature box;

3. Send the completed and signed DPA to us by email, indicating “*Client’s name – Signed DPA*” at the Subject line, to privacy@cynet.com; and
4. Cynet has received the validly completed and signed DPA via privacy@cynet.com; (the date of such receipt is the “**DPA Effective Date**”).

SCHEDULE 1 - DETAILS OF THE PROCESSING***Subject matter***

Cynet will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further instructed by Client in its use of the Services.

Nature and Purpose of Processing

1. Providing the Service(s) to Client.
2. Setting up profile(s) for users authorized by Clients.
3. For Client to be able to use the Services.
4. For Cynet to comply with documented reasonable instructions provided by Client where such instructions are consistent with the terms of the Agreement.
5. Performing the Agreement, this DPA and/or other contracts executed by the Parties.
6. Providing support and technical maintenance, if agreed in the Agreement.
7. Resolving disputes.
8. Enforcing the Agreement, this DPA and/or defending Cynet's rights.
9. Management of the Agreement, the DPA and/or other contracts executed by the Parties, including fees payment, account administration, accounting, tax, management, litigation; and
10. Complying with applicable laws and regulations, including for cooperating with local and foreign tax authorities, preventing fraud, money laundering and terrorist financing.
11. All tasks related with any of the above, including testing and improving the Services.

Duration of Processing

Subject to any Section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Cynet will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First name
- Last name
- Address
- Phone number
- Email address
- Hostname
- Username
- IP address
- Accessed URLs
- Files' names
- Any other Personal Data or information that the Client decides to provide to the Cynet or the Services.

The Client and the Data Subjects shall provide the Personal data to Cynet by supplying the Personal data to Cynet's Service.

In some limited circumstances Personal Data may also come from others sources, for example, in the case of anti-money laundering research, fraud detection or as required by applicable law. For clarity, Client shall always be deemed the “Data Controller” and Cynet shall always be deemed the “Data Processor” (as such terms are defined in the GDPR).

Categories of Data Subjects

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Client’s customers and/or clients
- Client’s users authorized by Client to use the Services
- Employees, agents, advisors, freelancers of Client (who are natural persons)
- Prospects, Clients, business partners and vendors of Client (who are natural persons)
- Employees or contact persons of Client’s prospects, Clients, business partners and vendors

SCHEDULE 2 – SUB-PROCESSOR LIST

Entity Name	Sub-Processing Activities	Entity Country
Cynet Group	Support, testing and R&D	US, Israel and UK
Amazon Web Services, Inc. and its affiliates	Cloud computing	For Cynet’s EU customers – Ireland. For Cynet’s customers located in the Americas – US.
Hubspot, Inc.	Email communication	US
Impartner, Inc.	Partner and Customer portal	US
Zoom Video Communications, Inc.	Video Conference	US
Microsoft Corporation	Email/Calendar	US/ The Netherlands
Oracle Corporation UK Limited	Finance platform	UK
Salesforce, Inc./SFDC Ireland Limited	CRM	US/Ireland
Delighted, LLC	Back-end product	US
Zimperium, Inc.	Mobile protection	US
Dealhub Ltd.	CPQ	Israel
Nooks Communications, Inc.	Telephone call automation	US
Coralogix Ltd.	Telemetry management	Israel
Vocalo Inc. (DBA “BoostUp.ai”)	Forecasting and pipeline management to improve forecast accuracy and deal health visibility	US
Docusign	Business operations	Ireland
Outreach Corporation	Sales engagement for sequences, emailing/calling workflows, and task automation. Tracks prospect engagement and rep activity	US
ZoomInfo	B2B company/contact intelligence, intent, and enrichment. Powers prospecting and data hygiene	US
Workato, Inc.	iPaaS automation platform to integrate apps and orchestrate workflows with triggers, recipes, and data sync. Reduces manual work and improves data consistency	Israel
Own Company	Backup/recovery for Salesforce data and metadata	US

SCHEDULE 3 – TECHNICAL AND ORGANIZATIONAL MEASURES

1	<p>Cynet will have in place System Security Solutions installed on all Cynet's IT devices used to access or store Client's information, including:</p> <ol style="list-style-type: none"> 1) Antimalware (incl. Antivirus / AntiSpyWare); 2) Firewall; 3) Network Access Control; 4) Removable device (e.g. USB) Encryption; 5) Host Intrusion Detection / Prevention; 6) Hard drive Encryption.
2	<p>Security updates (patches) are applied to relevant software and firmware storing or processing Client's information. These security updates are applied according to a structured patch management process</p>
3	<p>An encryption protocol is used for the sharing of Client's information over wireless networks (e.g., WPA, WPA2)</p>
4	<p>A procedure is in place to manage network threats, vulnerabilities and risks. Regular, periodic vulnerability and penetration testing (including internal network vulnerability testing) are performed.</p>
5	<p>Encryption practices are detailed either in an ad hoc policy or within the Information Security policy. Cryptographic key management rules and procedures are taken into consideration (including access controls, key restoration, maximum key life provisions).</p>
6	<p>Electronic transmissions of information are encrypted regardless of the location or format e.g., email.</p>
7	<p>A portable equipment use policy is in place, which requires users to safeguard information contained on portable media devices (e.g., laptops, hard drives, backup tapes, USB drives, memory sticks).</p>
8	<p>A mandatory secure destruction process is in place covering the destruction, at the end of their useful life or when broken/unusable, of the following:</p> <ol style="list-style-type: none"> 1) Hard drives; 2) PCs and Laptops; 3) Portable media e.g., DVD/CDs; 4) Paper; 5) Other devices with storage capability.
9	<p>End-users connecting their own devices (BYOD) to Cynet's IT environment processing Client's information have to ensure at least End-users' authentication before access.</p>

SCHEDULE 4 - STANDARD CONTRACTUAL CLAUSES

EU SCCs. If the Processing of Personal Data includes transfers from the EU to countries outside the EEA which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Chapter V of the GDPR. The Parties hereby agree to execute the Standard Contractual Clauses as follows:

- a) The Standard Contractual Clauses (Controller-to-Processor and Processor to Processor) if applicable, will apply, with respect to restricted transfers between Client and Cynet that are subject to the EU GDPR.
- b) The Parties agree that for the purpose of transfer of Personal Data between Client (as Data Exporter) and Cynet (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be applicable; (ii) In Clause 9, option 2 shall apply and the method described in Section 5 of the DPA (Authorization Regarding Sub-Processors) shall apply; (iii) Clause 11 of the Standard Contractual Clauses shall not be applicable; (iv) In Clause 13: the relevant option applicable to the Client, as informed by Client to Cynet; (v) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of the Republic of Ireland; and (vi) In Clause 18(b) the Parties choose the courts of Dublin, Ireland, as their choice of forum and jurisdiction.
- c) Annex I.A: With respect to Module Two: (i) Data Exporter is Client as a data controller and (ii) the Data Importer is Cynet as a data processor. With respect to Module Three: (i) Data Exporter is Client as a data processor and (ii) the Data Importer is Cynet as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this DPA, each Party is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.
- d) Annex I.B of the Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing) of this DPA.
- e) Annex I.C of the Standard Contractual Clauses shall be completed as follows: The competent supervisory authority is the Irish supervisory authority.
- f) Annex II of the Standard Contractual Clauses shall be completed as described and agreed between the parties in the Agreement and/or this DPA.
- g) Annex III of the Standard Contractual Clauses shall be completed with the authorized sub-processors detailed in Schedule 2 (Sub-processor list) of this DPA.

UK SCCs. If the Processing of Personal Data includes transfers from the UK to countries which do not offer adequate level of data protection or which have not been subject to an Adequacy Decision, the Parties shall comply with Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018. The Parties hereby agree to execute the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as follows:

- a) The UK Standard Contractual Clauses (Controller-to-Processor and Processor to Processor) if applicable, will apply with respect to restricted transfers between Client and Cynet that are subject to the UK GDPR.
- b) The Parties agree that for the purpose of transfer of Personal Data between Client (as Data Exporter) and Cynet (as Data Importer), the following shall apply: (i) Clause 7 of the Standard Contractual Clauses shall be applicable; (ii) In Clause 9, option 2 shall apply and the method described in Section 5 of the DPA (Authorization Regarding Sub-Processors) shall apply; (iii) Clause 11 of the Standard Contractual Clauses shall not be applicable; (iv) In Clause 17, option 1 shall apply. The Parties agree that the Standard Contractual Clauses shall be governed by the laws of England and Wales; and (v) In Clause 18(b) the Parties choose the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts, as their choice of forum and jurisdiction. Which Parties may end this Addendum as set out in Section 19: Importer and/or Exporter, in accordance with the agreed terms of the DPA.
- c) Annex I.A: With respect to Module Two: Data Exporter is Client as a data controller and the Data Importer is Cynet as a data processor. With respect to Module Three: Data Exporter is Client as a data processor and the Data Importer is Cynet as a data processor (sub-processor). Data Exporter and Data Importer Contact details: As detailed in the Agreement. Signature and Date: By entering into the Agreement and this DPA, each Party is deemed to have signed these UK Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the DPA.
- d) Annex I.B of the UK Standard Contractual Clauses shall be completed as described in Schedule 1 (Details of the Processing) of this DPA.
- e) Annex I.C of the UK Standard Contractual Clauses shall be completed as follows: The competent supervisory authority is the ICO supervisory authority.
- f) Annex II of the UK Standard Contractual Clauses shall be completed as described and agreed between the parties in the Agreement and/or this DPA.
- g) Annex III of the UK Standard Contractual Clauses shall be completed with the authorized sub-processors detailed in Schedule 2 (Sub-processor list) of this DPA.