DATA PROCESSING AGREEMENT

This data processing agreement (the "DPA") forms an integral part of the Outpost24 Master Agreement (the "Agreement") for provision of products and/or services entered into between the **customer or partner** (the "Controller"); and the relevant **Outpost24** company signing the Agreement (the "Processor"), to the extent such products and/or services comprise Processing of Personal Data by the Processor on behalf of the Controller.

1 Background and definitions

1.1 The EU General Data Protection Regulation 2016/679 (the "EU GDPR") and the Data Protection Act 2018 (the "UK GDPR") require a written agreement between a controller and a processor in order to allow the processing of Personal Data by the processor on behalf of the controller. For this reason, the parties have entered into this DPA as of the effective date of the Agreement.

1.2 Definitions

"Affiliate(s)" means in relation to Processor, a company or other entity which (a) is controlled, directly or indirectly, by Processor, (b) controls, directly or indirectly, Processor or (c) is under common control with Processor, who may Process Personal Data as a Sub-processor of Processor. Is controlled", "controls" and "is under common control with" shall be interpreted as referring to control of more than 50% of the voting power by virtue of ownership.

"Data Protection Laws" means the EU GDPR, the UK GDPR, and any national law of a European Union member state or United Kingdom law deriving from or supplementing the EU GDPR or the UK GDPR.

"Data Subject" means a natural person who can be identified, directly or indirectly, by the Personal Data.

"Personal Data" means any information relating to an identified or identifiable natural person, including an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" or "Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"SCC (s)" means, as applicable:

- For transfers subject to the EU GDPR, the standard contractual clauses between controllers and processors for the transfer of Personal Data, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, or any subsequent latest version thereof.
- For transfers subject to the UK GDPR, the International Data Transfer Agreement (IDTA) and/or the UK Addendum to the EU Standard Contractual Clauses, as approved by the Information Commissioner's Office (ICO) or any subsequent latest version thereof.

"Services" means the specific services provided by Processor to Controller as specified in the Agreement.

"Sub-processor" means any third party engaged by the Processor, or its Sub-processor, to Process Personal Data on behalf of the Controller.

2 Data processing

2.1 The Processor agrees to comply with Data Protection Laws, and with any other applicable law to the extent it is not in conflict with Data Protection Laws.

2.2 Unless otherwise specified in the Agreement, the Controller shall not provide the Processor with any sensitive or special Personal Data that imposes specific data security or data protection obligations on the Controller in addition to or different from those specified in this Data Processing Agreement.

2.3 The Processor shall only Process the Personal Data in accordance with the instructions stated in this DPA or any other written instructions provided by the Controller. If EU, UK or EU member state law imposes additional processing requirements, the Processor shall inform the Controller of such legal requirements before Processing, unless prohibited by applicable law on important grounds of public interest.

2.4 If the Processor lacks instructions which the Processor deems necessary in order to carry out an assignment from the Controller, or if the Controller's instructions to the knowledge of Processor, infringe Data Protection Laws or other applicable law, the Processor shall notify the Controller without undue delay and await the Controller's further instructions.

2.5 The Processor shall enable the Controller to access, rectify, erase, restrict and transmit the Personal Data Processed by the Processor. The Processor shall comply with any instructions in writing from the Controller related to the above without undue delay and in any event within fourteen (14) calendar days. If the Controller erases, or instructs the Processor to erase, any Personal Data held by the Processor, the Processor shall ensure that the Personal Data is erased so that it cannot be recreated by any party. In any event, Controller hereby allows Processor to delete the Personal Data remaining with Processor (if any) within a reasonable time period in line with Data Protection Laws and Processor retention policies (not to exceed twelve months) once Personal Data is no longer required for execution of the Agreement, unless applicable law requires retention.

2.6 The Processor shall notify the Controller without undue delay as to any contacts with a supervisory authority, concerning or of significance for, the Processing of Personal Data carried out on behalf of the Controller. The Processor may not represent the Controller, nor act on the Controller's behalf, against any supervisory authority or other third party.

2.7 The Processor shall provide reasonable assistance to the Controller in its contacts with any supervisory authority, including, upon the Controller's instruction, by providing any information requested by the supervisory authority. For the avoidance of doubt, the Processor may not disclose Personal Data or any information on the Processing of Personal Data without explicit instructions from the Controller.

2.8 If a Data Subject requests information from the Processor concerning the Processing of Personal Data, the Processor shall forward the request to the Controller and provide reasonable assistance to the Controller in responding to such request as obliged by Data Protection Laws. The Processor shall assist the Controller by appropriate technical and organisational measures, taking into account the nature of the Processing.

2.9 The Processor shall impose adequate contractual obligations regarding confidentiality and security upon its personnel which have been authorised to Process Personal Data.

2.10 The Processor shall provide reasonable assistance to the Controller in ensuring compliance with the Controller's obligations under Data Protection Laws, e.g. assist with security measures, data protection impact assessments (including prior consultation), and in situations involving Personal Data breach.

2.11 The Processor shall follow the Controller's written instructions and provide the reasonable assistance required within the timeframes reasonably necessary to allow Controller to comply with Data Protection Laws. To the extent that Processor expects to incur additional fees or charges not covered under the Agreement, it will promptly inform Controller thereof upon receiving its instructions. Without prejudice to the Processor's obligation to comply with the Controller's instructions, the Parties will then negotiate in good faith with respect to any such fees or charges.

2.12 If a Data Subject makes a request to the Processor under applicable Data Protection Laws, the Processor will promptly forward such request to the Controller once it has identified that the request is from a Data Subject for whom the Controller is responsible. The Controller expressly authorizes the Processor to respond to any Data Subject who makes such a request, to confirm that it has forwarded the request to the Controller.

2.13 The Processor shall maintain a record of all Processing activities carried out on behalf of the Controller. Upon the Controller's request, the Processor shall promptly make the record available to the Controller in a generally readable electronic format, including as a minimum the following information:

a) the name and contact details of the Processor, its authorized representatives, and if applicable, the data protection officer (as defined in Data Protection Laws) of the Processor;
b) where applicable, the name and contact details of any Sub-processor, an authorized representative, and, if applicable, the Data Protection Officer of the Sub-processor;
c) the actual processing activities carried out by the Processor and/or Sub-processor on behalf of the Controller;
d) where applicable, transfers of Personal Data to a third country including the identification of that third country and suitable safeguards employed to ensure an adequate level of protection of the Data Subject; and

e) a general description of the technical and organisational measures employed to ensure an appropriate level of security.

3 Security and Audit

3.1 The Processor shall implement appropriate technical and organisational security measures to protect the Personal Data in accordance with Data Protection Laws. The Processor shall particularly observe relevant codes of conduct, industry practice, and guidelines issued or approved by supervisory authorities.

3.2 The Processor shall notify the Controller, in writing, without undue delay, but no longer than 72 hours, after the Processor has become aware of any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data Processed for and on behalf of the Controller.

3.3 The Processor must be able to verify its compliance with this DPA and Data Protection Laws and shall maintain adequate documentation verifying fulfilment of its obligations hereunder. Further, the Controller may conduct audits to ensure that the Processor is complying with this DPA and Data Protection Laws. For such purpose, the Controller shall submit a detailed proposal of audit plan describing in detail the scope, duration, and proposed start date of the audit. The Processor will review the proposed audit plan and work cooperatively with the Controller to agree on a final audit plan. In any case, the audit shall be conducted on regular business hours and may not unreasonably interfere with the Processor's business activity.

3.4 Each party shall bear its own costs in relation to the audit, unless the Processor promptly informs the Controller upon reviewing the audit plan that it expects to incur additional fees or charges not covered under the Agreement in which case clause 2.11 above will apply.

3.5 Without prejudice to the rights granted in this clause, if the requested audit scope refers to ISO, SOC, NIST or equivalent rules and the Processor provides Controller with an audit report issued by a qualified third-party auditor within the prior twelve months confirming compliance with the controls audited, the Controller agrees to accept the findings presented in such third party audit report in lieu of requesting an audit of the same controls.

4 Sub-processing

4.1 The Controller hereby gives the Processor a general consent to engage Sub-processors, including current and future Affiliates of the Processor, for the purposes of Processing Personal Data on behalf of the Controller. The current list of Sub-processors is set out in Schedule 1. The Processor shall notify the Controller by email, addressed to a designated contact, of any intended change to the list of Sub-processors. The Controller may object to such change within ten (10) days of receipt of such notice on reasonable data protection grounds.

4.2 When a Sub-processor is engaged, the Processor (i) will restrict the Sub-processor's access to Personal Data only to what is necessary to provide or maintain the Services, and the Processor will prohibit the Sub-processor from accessing Personal Data for any other purpose; (ii) the Processor will enter into a written agreement with the Sub-processor imposing on the Sub-processor the same or equivalent contractual obligations that the Processor has under this DPA; and (iii) the Processor will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that may cause the Processor to breach any of its obligations under such DPA.

5 International Transfer of Personal Data outside of the EEA

5.1 If Processing of Personal Data under this DPA includes the International Transfer of Personal Data to a Sub-processor located in a country outside of the EEA or the UK which is not recognized by the European Commission or the UK ICO to have an adequate level of protection in accordance with Data Protection Laws, the Processor shall provide appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards will be provided by the execution of:

- For transfers outside the EEA, the SCC Module 3 which applies to international data transfers outside of the EEA from the Processor (the data exporter) to the Sub-processor (the data importer); and
- For transfers outside the UK, the UK IDTA and/or the UK Addendum to the EU SCCs.

5.2 If and to the extent this DPA and the SCC are inconsistent, the provisions of the SCC shall prevail. Moreover, and as a rule, the Processor shall not process or proceed with the International Transfer of Personal Data outside of the EEA or the UK, unless (i) this is absolutely necessary for the provision of the Services under the Agreement, and (ii) such an International Transfer is managed according to this clause.

5.3 To the extent such International Transfer of Personal Data outside of the EEA or the UK involves an Affiliate, the terms of the Outpost24 Intra-group Data Processing Agreement, which require all transfers of Personal Data to be made in compliance with applicable Data Protection Laws and to comply with the provisions of clause 5 herein, shall apply.

6 Term and termination

6.1 The DPA will enter into force upon the execution of the Agreement. Upon termination or expiry of the services relating to the Processing under the Agreement, upon written request by the Controller, the Processor shall submit all Personal Data to the Controller on a medium as reasonably requested by the Controller. The Processor shall thereafter, in accordance with the provisions on erasure in Section 2.5, ensure that there is no Personal Data remaining with the Processor or any of its Sub-processors.

6.2 This DPA is applicable from the date of its execution and until all Personal Data is erased in accordance with Section 6.1 above.

Schedule 1

This Schedule 1 constitutes the instructions regarding Processing of Personal Data by the Processor on behalf of the Controller. The instructions may be amended in writing by Controller from time to time.

1 CATEGORIES OF PERSONAL DATA PROCESSED

Depending on Controller's use of the Services, Processor may process the following types of personal data:

- Basic personal data: for example, first name. last name and email address;
- Authentication and login data such as usernames and passwords for accessing the Services, access times, access logs of files, addresses, comments;
- Contact information such as work email, address, cell phone and phone number;
- Unique device identifiers such as IP addresses;
- Any other personal data identified in Article 4 of the EU GDPR and/or UK GDPR, included in the systems and/or hardware of Controller to which the Controller at its own discretion is applying the Services, for example, Personal Information arising from Threat Intelligence Platform Services, web application scanning or Personal Data which is contained in Controller's log data, provided however that under clause 2.2 of this DPA, the Controller shall not provide the Processor with any sensitive or special Personal Data that imposes specific data security or data protection obligations.

2 CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS PROCESSED

The Personal Data Processed concerns the following categories of Data Subjects:

- Employees.
- Any other individuals such as contractors, subcontractors, temporary workers, agents and representatives to whom the Controller grants access to the Services.
- Other data and Data Subjects might be processed by Controller's choice in case of audits targeting specific systems or information sets, for example data leaks related to Controller's end users enlisted on a portal or data processed in an audited system.

3 SPECIAL CATEGORIES OF PERSONAL DATA

- Only applies to Specops Verified ID; information from a user's identity document and liveness selfie is transmitted over TLS in encrypted form to Specops cloud in Microsoft Azure. This data can be stored temporarily and deleted when no longer needed. It is typically removed immediately after the user has completed verification, and in all cases within 60 minutes. If user verification is unsuccessful, date of birth and names, can be saved up to 90 days for troubleshooting purposes.

4 PROCESSING OPERATIONS

- Storage and transfer: All data
- Analysis for security purposes: Log, access and monitoring
- Analysis and enrichment of data for Threat Intelligence Platform Services

5 NATURE OF THE PROCESSING

The nature of processing personal data is for Processor to provide the Services under the existing Agreement to Controller. This may include:

- Provision of Services: to provide Controller with the agreed Services in line with the governing Agreement;
- Ticket resolution: to communicate and co-ordinate resolution of support requests in a timely manner;
- Security and authentication: to identify and verify the identity of individuals related to Controller prior to providing access to systems and data and coordinate responses to potential information security events; and
- Systems administration: to ensure the availability and security of systems managed by Processor.

6 DURATION OF PROCESSING

The Personal Data will be processed for the duration of the Agreement, or the duration of any subsequent renewals of the Agreement, or for a retention period beyond the Agreement termination date of up to 12 months for auditing and security purposes, depending on Services provided, to which this DPA forms an appendix.

7 SUB-PROCESSORS

The Processor is using the sub-processors set out in the schedule below

8 SECURITY OF THE PROCESSING

Processor maintains a number of Technical and Organizational Security Measures ("TOMs") to ensure it processes and protects personal data in a responsible way, considering the types of Personal Data that it processes. The Processor is ISO 27001 and Cyber Essentials certified and conducts an external annual SOC 2 Type 2 report. An outline of the Processor's TOM's is available upon request.

SUB-PROCESSORS

Name of Sub-processor	Service provided	Location of processing
Cleura CityNetwork International AB	Processing of log and audit data for Outpost24 Group Vulnerability Management and application security products and services.	EU
Hetzner Online GmbH	Processing and storage of Outpost24 Group cyber threat intelligence products and services.	EU
Microsoft Azure	Hosting of Outpost 24 Group Access Risk (Specops) authentication service.	USA or EU (Controller can choose either)
Atlassian Corporation	Providing service desk portal on which Controller can make service requests, processed data will be limited to contact information and any information Controller chooses to post in the portal.	EU
Amazon Web Services	Processing and storage of Outpost24 Group vulnerability management, EASM, Threat Intelligence Platform Services and application security products and services.	EU
Twillio	SMS processing of Outpost 24 Group Access Risk (Specops) authentication service (optional service).	USA
Spirius AB	SMS processing of Outpost 24 Group authentication service (optional service).	EU

Sendgrid (part of Twillio)	E-mail processing of Outpost 24 Group Access Risk (Specops) authentication service (optional service – can be configured on premise)	USA
OVH	Processing and storage of Threat Intelligence Platform Services.	EU
Dynatrace	Processing of IP addresses when using Access Risk – Specops Authentication platform.	EU
SalesForce	Customer Relationship Manager for Outpost24 Group.	EU
Pendo	Processing account names, IP addresses, and country for user behavior analytics for ASM products and services. Other user data is anonymized prior to processing by Pendo. Customers may opt out of this usage monitoring at any time.	EU
Google Cloud	Cloud hosting platform for the SaaS solution for Infinipoint products and services.	USA or EU (Controller can choose either)
Google Firebase	Access Risk push notifications for Specops Fingerprint and Specops:ID (optional).	USA or EU (Based on Controllers choice of Microsoft Azure data center region)
Microsoft 365	Processing of contact information for internal usage within different Microsoft products such as Teams, Outlook and Sharepoint.	EU
Hubspot	Chat box within the Outpost24 EASM platform. This is not mandatory to use, it is an option for signed in users to create support tickets, ask questions etc.	EU
CGI Sverige	Identity verification brokering and transmission of end-user identity data from BankID and Freja eID to the Specops platform for authentication purpose (optional).	EU
Adobe Sign	Contracts signing portal	EU

Channeltivity	Platform for Outpost24 partner information, communication and deal registrations	USA