

Arctic Wolf's Product - Processing Details
(Last Updated: November 2024)

The Processing Details by Product below describe the applicable key details of the Personal Data Arctic Wolf processes as part of providing the applicable Product to our customers. These processing details may be updated by Arctic Wolf from time to time and will, to the extent required, notify customers of material changes.

Table of Contents

<i>Processing Details for Managed Detection and Response, Managed Risk, and Managed Security Awareness</i>	<i>2</i>
<i>Processing Details for IR JumpStart Retainer (IRJS), Cyber Defense Operations Services (CDO), Cyber JumpStart Portal, Incident Response Services (IR)</i>	<i>5</i>

Processing Details for Managed Detection and Response, Managed Risk, and Managed Security Awareness

A. LIST OF PARTIES

Data exporter(s):

Data exporter is the customer of data importer subscribing to the Solutions described in the Solutions Agreement executed by the parties for the delivery of managed detection and response and/or managed risk solutions.

Activities relevant to the data transferred under these Clauses:

Activities relevant to the data transferred under these Clauses: Data exporter is a business which processes Personal Data in the delivery of its services.

Data Exporter's role is Controller.

Data importer(s):

Data Importer is Arctic Wolf Networks, Inc., a provider of security operations solutions.

Address: 8939 Columbine Road, Suite 150, Eden Prairie, MN 55347

Contact person's name, position and contact details:

Pursuant to Article 27 of the UK GDPR, Arctic Wolf Networks, Inc. has appointed EDPO UK Ltd as its GDPR representative in the UK. You can contact EDPO UK regarding matters pertaining to the UK GDPR:

- by using EDPO's online request form: <https://edpo.com/uk-gdpr-data-request/>
- by writing to EDPO UK at 8 Northumberland Avenue, London WC2N 5BY, United Kingdom

Pursuant to Article 27 of the EEA GDPR, Arctic Wolf Networks, Inc. has appointed IITR Cert GmbH as its GDPR representative in the EEA. You can contact IITR Cert GmbH regarding matters pertaining to the EEA GDPR:

- by writing to IITR Cert GmbH, Dr. Sebastian Kraska, Data Protection Representative, Eschenrieder Str 62c, 82194 Groebenzell, Germany
- by email to email@iitr.de

Activities relevant to the data transferred under these Clauses:

Data importer is a vendor of data exporter and has contracted with data exporter for the delivery of data importer's security operation solutions which may require the processing of Personal Data and transfer of Personal Data to the US.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data Subjects include, but are not limited to, Solution users (Administrators), employees, contractors, agents, and other third parties

Categories of personal data transferred

Personal Data includes but is not limited to:

Contact information and information required to set up and deliver the Solutions: names, email addresses, postal address, phone numbers, user names, passwords, IP addresses, geolocation data, device ID.

Operational system log data provided by Data Exporter to Data Importer for the delivery of the Solutions, including, but not limited to operational values, event logs, and network data such as flow, HTTPS, TLS, DNS metadata, cursory inventory data, operating systems and versions, users and groups from Active Directory, system level inventory, event data, and network vulnerability data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The personal data transferred should not contain special categories of data, unless otherwise provided by Data Exporter.

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

Personal Data is transferred on an ongoing basis for the term of the Agreement.

Nature of the processing

The processing is as set forth in the governing Agreement executed by the Data Exporter and Data Importer as it pertains to the delivery of Data Importer's Managed Detection and Response and Managed Risk Solutions to the Data Importer.

Purpose(s) of the data transfer and further processing

Data Importer processes the Personal Data in accordance with the instructions of the Data Exporter as set forth in the Agreement and the Data Protection Addendum.

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

Contact information and information required to set up and perform the Solutions are retained during the Solutions subscription term for use in accordance with the Agreement.

Operational systems log data is retained for the retention period purchased by Data Exporter and returned or destroyed by Data Importer in accordance with the terms of the Agreement or as requested by Data Exporter.

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

Subprocessors process Personal Data to permit Data Importer's delivery of the Solutions to Data Exporter in accordance with the terms of the Agreement and are subject to terms and conditions, including terms related to duration of processing, no less restrictive than those required of Data Importer pursuant to the terms of the Agreement. The purpose of processing is set forth on Data Importer's subprocessor list.

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Supervisory Authority

Processing Details for IR JumpStart Retainer (IRJS), Cyber Defense Operations Services (CDO), Cyber JumpStart Portal, Incident Response Services (IR)

A. LIST OF PARTIES

Data exporter(s):

Data exporter is the Customer of data importer subscribing or purchasing, as appropriate, the Services described in the General Terms and reflected on an Order Form.

Activities relevant to the data transferred under these Clauses:

Activities relevant to the data transferred under these Clauses: Data exporter is a business which processes Personal Data in the delivery of the Services.

Data Exporter's role is Controller.

Data importer(s):

Data Importer is Arctic Wolf Networks, Inc., a provider of Services.

Address: 8939 Columbine Road, Suite 150, Eden Prairie, MN 55347

Contact person's name, position and contact details:

Pursuant to Article 27 of the UK GDPR, Arctic Wolf Networks, Inc. has appointed EDPO UK Ltd as its GDPR representative in the UK. You can contact EDPO UK regarding matters pertaining to the UK GDPR:

- by using EDPO's online request form: <https://edpo.com/uk-gdpr-data-request/>
- by writing to EDPO UK at 8 Northumberland Avenue, London WC2N 5BY, United Kingdom

Pursuant to Article 27 of the EEA GDPR, Arctic Wolf Networks, Inc. has appointed IITR Cert GmbH as its GDPR representative in the EEA. You can contact IITR Cert GmbH regarding matters pertaining to the EEA GDPR:

- by writing to IITR Cert GmbH, Dr. Sebastian Kraska, Data Protection Representative, Eschenrieder Str 62c, 82194 Groeben Zell, Germany
- by email to email@iitr.de

Activities relevant to the data transferred under these Clauses:

Data importer is a vendor of data exporter and has contracted with data exporter for the delivery of data importer's security operation solutions which may require the processing of Personal Data and transfer of Personal Data to the US.

Data Importer's role is Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data Subjects include data exporter's employees, contractors, agents, vendors, customers, and any such other persons with whom Controller transacts business and whose information is contained within the compromised systems, files and data provided to data importer for purposes of delivery of the Services.

Categories of personal data transferred

Personal Data includes names, email addresses, phone numbers, usernames, passwords, IP addresses, domain names, geolocation data, device ID, other system log metadata, business information,

emails, insurance policy numbers and limits, financial information which may include any category of Personal Data if Customer transmits such Personal Data to Arctic Wolf.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

For purposes of IR Services, Customer may provide Arctic Wolf with special categories of Personal Data, including protected health information, passport details, employment information, financial account information, and any other sensitive information which may be included in any compromised systems, files and data provided by Customer to Arctic Wolf for purposes of delivery of the IR Services.

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

Personal Data is transferred on an ongoing basis for the term of the Agreement.

Nature of the processing

The processing is as set forth in the governing Agreement executed by the Data Exporter and Data Importer as it pertains to the delivery of Data Importer's Services to the Data Exporter.

Purpose(s) of the data transfer and further processing

Data Importer processes the Personal Data in accordance with the instructions of the Data Exporter as set forth in the Agreement and the Data Protection Addendum.

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

Contact information and information required to set up and perform the Services are retained during the term of the Agreement for use in the administration and back-office processing of the Services engagement.

Incident Evidence, CDO Data, Points of Contact Information, and Security Profile Data (as defined in the applicable Agreement) will be returned or destroyed by Data Importer in accordance with the terms of such applicable Agreement.

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

Subprocessors process Personal Data to permit Data Importer's delivery of the Services to Data Exporter in accordance with the terms of the Agreement and are subject to terms and conditions, including terms related to duration of processing, no less restrictive than those required of Data Importer pursuant to the terms of the Agreement. The purpose of processing is set forth on Data Importer's subprocessor list.

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Supervisory Authority