

Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

ICSP Neural

This Privacy Transparency Notice describes how ICSP Neural (“Product”) collects and processes Personal Data. Its purpose is to provide You (our current or prospective “Customer”) the information You need to assess the Personal Data processing that is involved in using the Product.

1. Product Description

The Symantec Industrial Control System Protection (ICSP) Neural is a self-contained aluminum unibody USB Scanning Station that scans, detects and protects critical IOT environments from USB-borne malware traversing the air-gap. For secure media transfer, the scanning station leverages and visualizes Symantec’s most advanced threat protection machine learning cross-hatched with signatures, emulation and reputation to help protect the Customer against weaponized malware.

Further information about the Product is available at:

<https://www.symantec.com/products/industrial-control-system-protection-neural>

2. Personal Data Collection And Processing

Sources of Data

The Product only collects data from removable media which the Customer connects to it.

Respective Roles of Symantec and Customer

The Product is deployed on-premise in the Customer’s environment and does not transmit any Personal Data to Symantec or to any third party. The Customer is the sole Controller of any Personal Data on removable media which connects to the Product.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Network identifiers of devices in the Customer’s industrial control environment	Customer end-users	Identification of industrial control system components within the Customer’s environment

The Product does not need and is not meant to collect or process any Special Categories of Personal Data.

Personal Data Retention Schedule

The device does not retain any Personal Data.

3. Disclosure and International Transfer of Personal Data

Recipients of Personal Data

All data collected and processed by the device remains within the Customer’s environment.

Third-Party Sub-Processors

No third-party sub-processor is involved in delivering the Product.

4. Exercise Of Data Subject Rights

The device neither collects, nor processes any Personal Data susceptible of being covered by any Data Subjects' rights such as the rights of access, rectification, deletion and objection laid down in Chapter III of the EU General Data Protection Regulation (GDPR).

5. Information Security

Technical and Organizational Measures

It is Symantec's and all of its affiliated entities' commitment to implement, and contractually require all sub-processors to implement, appropriate technical and organizational measures to ensure an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of Data Subjects. Additional security documentation is available on the [Symantec Customer Trust Portal](#).

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Product. It supersedes any prior Symantec communication or documentation relating thereto.