Cysiv Privacy Policy - Customers

At Cysiv we respect and protect the privacy of the data our customers and employees entrust to us.

This Privacy Policy explains our privacy practices and how we handle the information we process for both our customers and data subjects.

Cysiv strives to follow these concepts when it processes personal information:

1. **Transparency**. We tell you what we are collecting. We disclose any subprocessors that we use to provide the service. We do not give, sell, rent, or loan personal information to third parties.
2. **Purpose Limitation.** We process personal information for the reasons that we tell you when collecting it. We collect what is necessary to fulfill that purpose. We retain the data only as long as necessary then securely delete it.
3. **Security.** We take reasonable and appropriate measures to protect personal information.
4. **Individual rights**. Where appropriate, we provide you with access to your personal information and allow you to exercise your rights in that information including the ability to see, correct and delete this information.

If you have a request, feedback or suggestions on our Privacy Policy, please email Cysiv's Compliancy and Data Protection Officer: Angus MacDonald at compliance@cysiv.com

Personal Information Cysiv collects and processes, how, why, what do we do with it, and for how long.

Cysiv practices Privacy by Design and Privacy by Default in the design, development and operations of our services. We strive to collect the minimum amount of personal information necessary and to retain it no longer than necessary to meet our contractual obligations or as required by law.

Cysiv Advanced Managed Security Service (AMSS)

Cysiv is a Data Processor that provides an Advanced Managed Security Service (AMSS) for customer organizations (i.e. Data Controllers, Covered Entities) looking to improve their overall security posture. In order to perform this service, we collect data from customer's security and system logs that we process and analyze for indicators of compromise and malicious behavior. Customers decide what logs to provide to Cysiv and can discontinue any or all feeds at any time.

The following personal data may be collected depending on what services are being provided under contract by Cysiv, what logs are being sent to Cysiv by the customer and which fields the customer has enabled:

- **Email**: recipient address, sender address, email subject,
- **User**: directory information may include unique userID, username, email address, user distinguished name, organizational unit, employee ID
- **Endpoint**: IP address, local user accounts, hostname of endpoint, MAC address of endpoint, endpoint owner name, location

Unless required contractually, these logs are kept a maximum of 12 months and are then securely deleted.

Personal Sensitive Data

Cysiv does not seek to collect any sensitive data through the service (e.g. health or credit card or other sensitive information). It is possible that as a result of malicious activity by a user or system that limited amounts of sensitive data may be contained in security logs sent to Cysiv. If such sensitive data is discovered Cysiv will securely delete it. If this continues to be an issue, Cysiv will notify the customer and together will take appropriate steps to prevent such information from being sent to Cysiv.

Cysiv understands that given the nature of our business, our customers, the type and volumes of data we're processing that limited amounts of personal sensitive data may be ingested and stored in our system therefore we apply the appropriate security controls and procedures with that assumption in mind e.g. firewalls, role-based access controls, antimalware products, encryption etc.

Legal Basis for Processing

Cysiv processes personal data based on several different legal basis, including but not limited to:

- Performance of a contract;
- Processing s necessary to protect vital interests;
- Consent of the data subject;
- as necessary for our legitimate interests in providing various services where those interests do not override your fundamental rights and freedoms related to data privacy

GDPR and Data Subject Rights

If you are a citizen of the EU and have any questions, comments or wish to make a request under GDPR please contact our GDPR Data Privacy Officer Lianne Harcup at GDPR@trendmicro.com

As Cysiv has no relationship with the data subjects themselves and would have difficulty authenticating any direct requests; employees or customers of Cysiv's corporate customers who wish to review, correct, or delete their personal information must make their request to their employer or service provider who has contracted Cysiv who will then review the request and instruct Cysiv accordingly. Cysiv will respond to such request in a timely manner and to the best of our abilities. All such requests will be logged, tracked and auditable.

1. Right to Access Personal Data - Through our Cysiv Command Portal, Cysiv's customers can query the logs index for events processed for a specific src_host, src_ip or user_name or they can make a request to Cysiv to perform the query. The query will return events indexed in the last ~31 days. Up to 4000 query results at a time can be exported to CSV. If events are collected for the data subject > 31 days, customer will first need to perform a restore for the timeframe

processing occurred for the data subject Cysiv can provide information collected about a data subject to the customer who will then determine what can or cannot be shared.

2. Right to Rectification – Cysiv only collects system and security logs which are an accurate snapshot of the system at a point in time regardless if the data subject's information is correct or not therefore, we would not make changes to log data collected.

3. Right to Erasure – Erasure of information from system or security logs is not generally supported as this would invalidate the integrity of the logs. Requests for erasure will be reviewed by Cysiv's DPO.

4. Right to Restrict Data Processing – In response to such a request, customers can restrict / filter the data they provide to Cysiv. Given the nature of the work Cysiv does on behalf of a customer, restricting data processing could expose the customer, their business or the data subject to a security risk.

5. Right to be Notified – Cysiv works with our customers (Data Controllers) to ensure that they understand the data being collected and why and can communicate this clearly with their data subjects.

6. Right to Data Portability – Cysiv does not store customer records but only system and security logs which would not support data portability to non Cysiv applications however the Cysiv Client can query the log index for events and provide to data subject in the form of a CSV file if desired.

7. Right to Object – Cysiv will work with the Data Controller on any such request.

8. Right to Reject Automated Individual Decision-Making – Cysiv employs automated technologies such as artificial intelligence and machine learning to analyze system and security logs for indications of suspicious and/or malicious behavior. This information could be used by a customer as part of their security controls to automatically block a threat vector or to quarantine a system or endpoint. Allowing data subjects to reject this automation could open data controllers up to unacceptable cyber risks and would not be supported.

9. Right to file a complaint with supervisory authorities – Data subjects may file a complaint with the appropriate supervisory authority. Cysiv will work with the Data Controller and supervisory authority to resolve any issues or complaints to the best of our ability.

Health Information Portability and Accountability Act (HIPAA)

This Privacy Policy explains our privacy practices and how we handle the information we process for our customers with respect to Health Information Portability and Accountability Act (HIPAA) and Protected Healthcare Information (PHI)

Protected health information (PHI) under the US law is any information about health status, provision of health care, or payment for health care that is created or

collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

While Cysiv collects personal identifiers such as names, email addresses, IP and device addresses from system and security logs for analysis of malicious or suspicious cyber activity, we do not collect any information about health status, provision of health care, or payment for health care services.

Under certain circumstances the data collected could be considered PHI. As an example, a small hospital or clinic could be identified by the naming of their security device. This device name when combined in the logs with a patient username, URL or IP address could be considered PHI. The more specific the services of the hospital or clinic the more sensitive would be the nature of the PHI. On the other hand, a security device name from a large payor when combined in the logs with a patient name, URL or IP address could be considered far less sensitive as there would be no additional information about the health status, provision of health care, or payment for heath care nor could such information be realistically inferred from the name of the payor.

Cysiv's customers (Covered Entities) have full control over which individual system or log fields they are willing to provide based on the service/s being provided. Individual field attributes can be removed altogether, or regex expressions can be applied to filter out known data string formats such as unique patient identifiers.

Cysiv is a Business Associate and will as required enter into a Business Associate Agreement with our Covered Entity customers and Business Associate third party suppliers.

HIPAA and Patient Rights

By law, the HIPAA Privacy Rule applies only to covered entities. Cysiv is not a covered entity and only processes data from a covered entity based on terms and conditions outlined in a business associate agreement. Cysiv will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule

Cysiv Command Portal

Cysiv customers and Cysiv employees' or contractors' access Cysiv's web-based next-gen SIEM, Cysiv Command, to review logs, detections, cases, dashboards and to perform other administrative functions. Access is controlled by role-based user accounts so that users can only access data that they're authorized to see.

The following personal data may be collected as part of Cysiv Command user account creation and management:

- User name
- Email address

- Country

User accounts are deleted when no longer required. User account information captured in Cysiv Command logs e.g. logins, searches etc., are kept for 12 months and rolled over.

A user can see, modify and delete their user account and log information if they have appropriate privilege otherwise, they can make such request to their Company admin or directly to Cysiv. All such requests will be logged, tracked and auditable.

Who Does Cysiv Share Personal Information With?

Cysiv uses sub-processors to assist with the delivery of the Service. These sub-processors have access to personal information only to assist Cysiv to process that data as authorized. All sub-processors are subject to a check in which Cysiv reviews privacy, security, and confidentiality practices. Cysiv currently uses the following sub-processors to assist it in providing its services:

Cysiv Advanced Managed Security Service (AMSS)
- Google Cloud Platform (all customer data is encrypted from Google)

Cysiv Command Portal
- Google Cloud Platform (all customer data is encrypted from Google)
- AuthO

We Take Our Data Protection Obligations Extremely Seriously!

Cysiv is committed to ensuring the security of personal information through reasonable and appropriate measures to protect it from loss, misuse, and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

We utilize industry security best practices to protect the confidentiality and security of personal information within the Service, by employing technological, physical and administrative security safeguards, such as firewalls, encryption, and other security procedures. These technologies, procedures, and other measures are used to ensure that customer data is safe, secure, and only available to those authorized to access the data. Specifically, we use tools and procedures to restrict access to and disclosure of personal data, obtain assurances from third party information security service providers, secure our networks and physical facilities and ensure management oversight of operations.

International Data Transfers

Cysiv receives and processes personal data from clients and may transfer, process and store personal information outside of the European Union to wherever we or our third-party service providers operate. Cysiv takes the appropriate methods to protect personal data whenever data is transferred from the EU to another location. Specifically, Cysiv employs the EU Controller to Processor Model Contract Clauses (MCC) in our Data Processing Addendum as Cysiv's

transfer mechanism for personal data. The terms of the SCCs apply where the transfer of Customer Personal Data from the EU to Cysiv.

Use of Cookies and Other Tracking Technology

Cysiv Command Portal uses cookies to maintain your session. It doesn't use beacons, analytics software, ad software, tracking software, or any other software that keeps a record of user behavior. If we do add analytics software in the future, then we would make sure to respond to Do Not Track an notify the users of the use of cookies appropriately.

Cysiv's Official website, www.cysiv.com, online services, interactive applications and email messages may use the following:

- "cookies" and other technologies such as web beacons. Cookies are alphanumeric identifiers that Cysiv transfers to your computer's hard drive through your web browser to enable our systems to recognize your browser to provide services. Cookies help websites work or work more efficiently and can help provide us with business and marketing information. They also enable a website to tailor information presented to you based on your browsing preferences such as language and geographical region.
- Cysiv may use cookies to personalize web pages during your visit to our web sites; and/or remember you for easy navigation and access during return visits after registering for product and service information, sales contacts and other offers including but not limited to White papers, webcasts, events, evaluation software, etc., provide information about the previous link used by you, track your visits to our website, aggregate and analyze data about your machine, such as browser type, screen resolution, operating system. This information, which does not personally identify you, is used to determine what content to serve to you when you land on our pages. The data collected by the cookie expires after 14 days unless you visit our website again.
- If you do not want Cysiv to deploy cookies in your browser, you can set your browser to reject cookies or to notify you when a website tries to put a cookie in your browser software. Rejecting cookies may affect your ability to use of some of our products and/or services.

Cysiv Privacy Policy – Employees and Contractors

At Cysiv we respect and protect the privacy of the data our customers and employees entrust to us.

This Privacy Policy explains our privacy practices and how we handle the information we process for both our employees and contractors.

Cysiv strives to follow these concepts when it processes personal information:

1. **Transparency.** We tell you what we are collecting. We disclose any subprocessors that we use to provide the service. We do not give, sell, rent, or loan personal information to third parties.
2. **Purpose Limitation.** We process personal information for the reasons that we tell you when collecting it. We collect what is necessary to fulfill that purpose. We retain the data only as long as necessary then securely delete it.
3. **Security.** We take reasonable and appropriate measures to protect personal information.
4. **Individual rights**. Where appropriate, we provide you with access to your personal information and allow you to exercise your rights in that information including the ability to see, correct and delete this information.

If you have a request, feedback or suggestions on our Privacy Policy, please email Cysiv's Compliance and Data Protection Officer: Angus MacDonald at compliance@cysiv.com. If you are a citizen of the EU and have any questions, comments or wish to make a request under GDPR please contact our GDPR Data Privacy Officer at GDPR@trendmicro.com

Cysiv employees and contractors should also refer to "Cysiv's Privacy Policy – Customers" for information about their account information privacy in Cysiv Command Portal.

Legal Basis for Processing

Cysiv like any other company must collect personal and sometimes sensitive information from employees in order to support business functions such as: corporate email, human resource and pay systems, internal collaboration applications etc. Cysiv processes personal data based on several different legal basis, including but not limited to:

- You have given consent
- processing is necessary for compliance with a legal obligation to which Cysiv is subject;
- processing is necessary in order to protect the vital interests of the Cysiv employees
- processing is necessary for the purposes of the legitimate interests pursued by Cysiv, except where such interests are overridden by the interests or fundamental rights and freedoms of employees

Our intention is to not keep any personal data longer than necessary and to only keep the minimum required to do our jobs or by law.

The following personal data may be collected from Cysiv employees or contractors as part of Cysiv's condition of employment:

- Employee information: name, D.O.B, phone numbers, address, employment history, pay information, other HR related information as required by law

- Next of kin / contact, relationship, phone numbers, address

User account information will be deactivated when no longer required and retained based on system backup and retention policies. Human resource information will be retained in accordance with applicable laws governing the storage and retention of such data.

Employees or contractors wishing to review, modify or delete their personal account information or HR information can make a request directly to Cysiv HR who will review the request and direct IT to take the appropriate action based on legal requirements.

Cysiv may disclose personal information in response to subpoenas, court orders, legal process, lawful requests by public authorities (including to meet national security or law enforcement requirements), or to establish or exercise our legal rights or defend against legal claims. We may also share such information if we believe it is necessary in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Service, or as otherwise required by law.

Who Does Cysiv Share Personal Information With?

Cysiv uses sub-processors to assist with the delivery of our corporate services. All sub-processors are subject to a check in which Cysiv reviews privacy, security, and confidentiality practices.

Cysiv is a Trend Micro Associate. Trend Micro provides business support services to Cysiv including IT, Finance, HR, and Facilities and therefore will have access to Cysiv employee and contractor information. Trend Micro follows the same or equivalent privacy and security guidelines as Cysiv.

Cysiv Internal Systems (not all apply to all employees / contractors)

- Cysiv Command
- Microsoft O365
- ADP
- Slack
- Zoom
- ExpensAble
- Carlson Wagonlit
- Github
- Jira
- Jenkins

We Take Our Data Protection Obligations Extremely Seriously!

Cysiv is committed to ensuring the security of personal information through reasonable and appropriate measures to protect it from loss, misuse, and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

We utilize industry security best practices to protect the confidentiality and security of personal information within the Service, by employing technological, physical and administrative security safeguards, such as firewalls, encryption, and other security procedures. These technologies, procedures, and other measures are used in an effort to ensure that customer data is safe, secure, and only available to those authorized to access the data. Specifically, we use tools and procedures to restrict access to and disclosure of personal data, obtain assurances from third party information security service providers, secure our networks and physical facilities and ensure management oversight of operations.