White Paper

Compliance of Trend Micro's Customer Support with the EU General Data Protection Regulation (GDPR)

I. Executive Summary

Trend Micro recognizes that the General Data Protection Regulation (GDPR) is an essential step in strengthening the individual's rights in the digital age and has a program in place which incorporates the requirements under the GDPR.

Trend Micro's Customer Support, including Trend Micro's Premium Support Program (PSP), onsite escalation management, and Trend Micro™ Managed XDR service **can be used by customers in compliance with German and European data protection law, in particular the GDPR**:

- Trend Micro acknowledges the **data ownership of the customer,** which means that the **customer has full control of the personal data** provided to Trend Micro's Customer Support. To this end, Trend Micro and the customer enter into a **Data Processing Addendum,** according to which the customer is the data controller, and when providing Customer Support, Trend Micro acts as data processor.
- Trend Micro has established an **interlocking contractual structure of data processing agreements within the Trend Micro group of companies and with subcontractors. These agreements** ensure personal data provided or disclosed in the course of Trend Micro's Customer Support will only be transferred to Trend Micro entities and subcontractors of Trend Micro in third countries, if an adequate level of data protection is ensured.
- As far as **customer data**, in particular contact records, it will be collected and processed by Trend Micro for providing and invoicing Trend Micro Customer Support to the customer, and thus its processing is **necessary for the performance of Trend Micro's Customer Support contract** vis-à-vis the customer.
- The **collection and processing of personal data by Trend Micro's Customer Support, for the purposes of ensuring network and information security,** can be considered as being **necessary for the purposes of the legitimate interests pursued by the customer and by third parties,** and thus as **lawful**.
- Trend Micro adheres to the **principles of the GDPR,** and in particular, has implemented appropriate **technical and organizational measures (TOM)** to **ensure integrity and confidentiality** of the personal data of the customer.

II. Data collected and processed by Trend Micro's Customer Support

Trend Micro's commercial Customer Support operation strives to deliver a top-quality level of service, while always recognizing that how the customer's personal data is processed is also critically important.

1. Components of Trend Micro's Customer Support

Some **components of the Customer Support** organization are:

- 24x7 global customer facing team (hubs in Europe, USA, and Asia)
- Support of product issues and queries
- Support of threat issues
- PSP
- Onsite escalation management, based on a statement of work (SoW)
- Managed detection and response service (Managed XDR service)

In the following, Trend Micro's Customer Support shall be explained in more detail and it will be examined how **customers can use Trend Micro's Customer Support in compliance with the GDPR**. It will also be elaborated that **Trend Micro acts as a processor** in the means of the GDPR, on what legal basis personal data will be transferred within the Trend Micro group of companies and to subcontractors of Trend Micro, and which technical, organizational, and additional security measures Trend Micro has implemented.

2. Customer data

Trend Micro customers using Trend Micro's Customer Support usually open a new **support ticket** via Trend Micro's primary Customer Relationship Management (CRM) platform: Salesforce. Typically, the **contact record** contains the following **personal data of employees of the customer** who use the support service: Salutation, first name, last name, job function, work address (being necessary in case of onsite support), work email, and work phone number. Additional contact details, such as mobile phone, fax number, or remote session ID, can be submitted as the preferred method the employee wants to be contacted. Additional data collected will be the device ID, operating system, MAC address, and public IP address of the user's gateway to the internet, as well as the license key and product information, in order to verify the customer's license and to individualize the requested support service to the customer's system architecture. Further, the service request or activity information submitted to Trend Micro will be collected.

Trend Micro employees supporting a customer who opened a support ticket have access to the contact records of such customer. If they login remotely, they access the same information, which will be adequately secured and encrypted in transit by VPN. **All of this personal data from the customer will be processed for the performance of the Trend Micro Customer Support contract vis-à-vis the customer.**

3. Customer Support

Trend Micro will appoint a **Customer Service Manager (CSM)** to serve as the principal contact with Trend Micro and can be located at the customer's premises, at a Trend Micro service center, or remote, depending on the region where the customer is located. The CSM will develop an understanding of the customer's system architecture, software, and hardware configuration based on the information provided by the customer; and will coordinate customer requests for technical support. Trend Micro's Technical Support Centre of Excellence is staffed with a team of **Customer Service Engineers (CSE)** that will assist support customers with technical product issues. Customer support may include **guidance and advice** in connection with customer's efforts to install, configure, and deploy Trend Micro products, status meetings, onsite visits, **periodic health checks,** and **security assessments**.

Other support services provide **proactive antivirus support,** where Trend Micro informs the customer about new threats of designated risk ratings based on the risk level pre-selected by the customer and **advanced malware incident assistance.** In the event of an internal malware outbreak, the customer will receive information on the infection threat, steps on mitigating further infection risk, eradication procedures, and recommendations on preventing future infections. In the event of a **critical virus infection case**, the case will be escalated to a dedicated Trend Micro antivirus engineer or to the Trend Micro antivirus escalation engineering group for resolution. Via the CSM, the antivirus engineering group will provide the customer with periodic status reports.

Trend Micro also offers **onsite escalation management** based on a SoW.

4. Managed Detection and Response (Managed XDR Service)

The managed detection and response service (Managed XDR service) of Trend Micro is a service where Trend Micro provides detection and response services on behalf of its customers. Managed detection and response monitors data from customers' email, endpoints, servers, cloud workloads, and networks 24/7, and uses advanced analytics and artificial intelligence (AI) techniques to correlate and prioritize alerts according to severity. Customers have access to **Trend Micro threat experts** who can provide **actionable remediation plans** and **guidance**. They also perform a **root cause analysis** to get a understanding of how attacks are initiated, how far they spread, and what remediation steps need to be taken. For this purpose, Managed XDR collects data from endpoints, network security, and server security, in order to correlate and prioritize alerts and system information, determine a root cause analysis, and provide advanced **threat hunting** and respective **reporting of investigated critical events** to the customer. In the case of a critical event, Trend Micro experts get access to this data to provide the Managed XDR service to the customer. Usually, only data from the endpoints is accesed, but the content

of the traffic between endpoints, such as files, will not be collected by the Managed XDR service to avoid identifying individuals, in particular, employees of the customer.

For more information, please see the **Trend Micro Managed XDR White Paper,** which can be retrieved here: https://www.trendmicro.com/en_us/business/campaigns/art-of-cybersecurity/it-security/user-protection/managed-xdr-white-paper.html.

5. Access of Trend Micro to Personal Data

A CSM, CSE, antivirus engineers (if necessary), the Trend Micro antivirus escalation engineering group, and Managed XDR experts might access **personal data of individuals contained in files, emails, or other information,** which will be provided or made available to Trend Micro in the course of providing Customer Support. Such personal data could be part of virus cases, service requests, or support tickets of the customer. The personal information could include IP addresses and URLs of websites visited, senders, recipients, and contents of suspicious emails and attachments to emails, behavior of applications and of users, metadata of devices and from suspicious executable files, detected malicious network connection information, debug logs, network architecture/topology, or a screen capture of errors. As well, it could include **data collected by the Managed XDR service** from endpoints, network security, and server security, such as host IP addresses, email addresses, files accessed, or traffic connections.

In order for Trend Micro to provide Customer Support, the customer has to grant Trend Micro **full access to their system environment**, and for onsite support **access, to the their business premises**.

Occasionally, customers may need to send in **dump files for threat/malware analysis** that could include personal data. A “dump file” is a snapshot of a live process containing information about its current state (including memory, stack traces, thread information, and module information, but no content information), which allows Trend Micro to inspect this snapshot of the process. A dump file is often generated when a process is about to crash due to an unhandled exception, but can be taken at any point. Dump files can contain personal data, such as a computer name or IP address, in order to troubleshoot the technical issue. The customer should either delete or anonymize all personal data in the dump file before submitting to Trend Micro.

Such personal data usually does not contain any special categories of personal data–also called **“sensitive data”**–such as political opinions or sexual orientation. Customers are advised to refrain from providing such sensitive data to Trend Micro, since Trend Micro neither wishes to receive nor needs any such sensitive data. However, it cannot be excluded if the sensitive data is contained in suspicious emails or files provided to Trend Micro by the customer for inspection.

It shall be noted that for all its products and services, including the Managed XDR, Trend Micro provides a **data collection disclosure** on what kind of data a Trend Micro product collects and how the customer can **opt-out of the data collection**. The data collection disclosure can be accessed here: https://success.trendmicro.com/data-collection-disclosure, and for Managed XDR here: https://success.trendmicro.com/solution/1122115.

This White Paper deals with the compliance of Trend Micro's Customer Support with the GDPR. Such support will only be provided in connection with products or services of Trend Micro, such as Trend Micro Apex One™ or the Trend Micro™ Smart Protection Network™, which also collect and process personal data. Trend Micro has published various White Papers explaining privacy issues of its products and services, which can be found on the Trend Micro website: https://www.trendmicro.com/en_us/about/legal/privacy-whitepapers.html

III. COMPLIANCE WITH THE GDPR

1. Customer Being Controller and Trend Micro Being a Processor or Sub-Processor Pursuant to a Data Processing Addendum

Trend Micro acknowledges the **data ownership of the customer,** which means that the customer has full control of the personal data provided to Trend Micro's Customer Support. Meaning, the **customer is the data controller,** and when providing Customer Support, **Trend Micro acts as data processor** and allows the customers to retrieve or delete their personal data, if needed. Trend Micro and the customer enter into a **Data Processing Addendum (DPA),** which applies to the extent that Trend Micro processes any personal data governed by the GDPR, in connection with providing any Customer Support to the customer as processor or sub-processor for the customer. The DPA forms part of any Trend Micro agreement that incorporates this DPA by reference, such as the PSP Agreement, and can be retrieved here: https://www.trendmicro.com/en_us/about/legal/data-processing-addendum.html.

The **Standard Contractual Clauses** of the European Union (EU), regarding the transfer of personal data to processors established in third countries, which do not ensure an adequate level of data protection, are incorporated in the DPA. Under these "Standard Contractual Clauses", a customer located in the EU will be regarded as the data exporter and the controller who transfers personal data to Trend Micro Incorporated, located in the USA, will be regarded as the data importer and the processor, who processes personal data for the purpose of providing Trend Micro Customer Support on behalf of the customer. By means of these Standard Contractual Clauses, an adequate level of protection of personal data transferred from the EU to Trend Micro Incorporated in the USA is ensured and **the transfer of personal data to Trend Micro Incorporated is permissible**.

Trend Micro Incorporated being the data importer is in turn allowed under the EU Standard Contractual Clauses (processors) to subcontract any of its processing operations performed on behalf of the customer to sub-processors, provided that the obligations of the Standard Contractual Clauses will also be imposed on the sub-processor. Trend Micro and its subcontractors have adhered to these requirements, since any **transfer of personal data within the Trend Micro group and to subcontractors of Trend Micro** will be safeguarded by the Global Intra-group Data Transfer Agreement (IGA) of Trend Micro, data processing agreements with subcontractors, and by using Standard Contractual Clauses. Trend Micro has established an **interlocking contractual structure of data processing agreements. This** ensures that the customer maintains data ownership, can exercise their rights as controller, and that the personal data provided or disclosed in the course of Trend Micro's Customer Support will only be transferred to Trend Micro entities and subcontractors of Trend Micro in third countries, if an adequate level of data protection is ensured.

It shall be noted that customers, which are receiving Trend Micro Customer Support on behalf of their **affiliates,** must ensure within their group of companies that the customer may contract Trend Micro Customer Support on behalf of its affiliate, for instance, by means of a respective data processing agreement. In such case, the affiliate will be the controller, the customer will be the processor, and Trend Micro acts as sub-processor.

2. Transfer of Personal Data Within the Trend Micro Group of Companies

When providing Trend Micro Customer Support, personal data from customers located in the EU will not only be collected and processed by a Trend Micro entity also located in the EU. It will also be collected and processed by **Trend Micro Incorporated located in the USA** and other Trend Micro entities in various countries, since **Trend Micro support teams operate worldwide**. In order to allow the transfer of personal data within the worldwide Trend Micro group of companies, all entities of the multinational Trend Micro group have entered into a **"Global Intra-group Data Transfer Agreement". This allows** the data to be used by Trend Micro for its own purpose and data processed by the transferring Trend Micro entity on behalf of its customer, as a processor, so that the receiving Trend Micro entity acts as sub-processor. This Global Intra-group Data Transfer Agreement incorporates the Standard Contractual Clauses of the EU for both the controller to controller and the controller to processor transfer–as the case may be–to third countries, which do not ensure an adequate level of data protection. By means of this Global Intra-group Data Transfer Agreement, in connection with the applicable Standard Contractual Clauses, an **adequate level of protection of personal data transferred within the Trend Micro group to Trend Micro entities located outside the EU is ensured** and the respective transfer is legitimate.

3. Transfer of Personal Data to Subcontractors of Trend Micro

Trend Micro uses Salesforce as their primary CRM platform. This includes an internal case-handling system and external-facing support portals. Trend Micro runs a global instance of

Salesforce, hosted in the United States, across the organization. Any customer files gathered to support a technical issue are stored securely on an internal file repository. This platform is hosted on Amazon Web Services (AWS) in Japan and accessed via the CRM. Trend Micro does not intentionally capture personal data on any other internal tools or systems.

Trend Micro has entered into respective **Data Processing Agreements with Salesforce and AWS,** which allows the processing of personal data by these providers as subcontractors of Trend Micro. These Data Processing Agreements *inter alia* ensure that the subcontractor will process customer data only in accordance with Trend Micro's instruction, and in turn, Trend Micro will follow the instructions of its customers. The subcontractor has also implemented and will maintain robust technical and organizational measures and that the subcontractor will notify Trend Micro of a security incident without undue delay, so that Trend Micro can inform the customer accordingly and the customer will comply with his **data breach notification obligations** under the GDPR. Further, these Data Processing Agreements include **Standard Contractual Clauses** so that an adequate level of protection of personal data transferred from the EU to the USA is ensured and the **transfer of personal data to Salesforce and AWS in the United States is permissible**.

In terms of the hosting of data on **AWS in Japan,** it shall be pointed out that according to the adequacy decision of the European Commission from 23 January 2019, **Japan ensures an adequate level of protection of personal data** transferred from the EU to business operators in Japan, so that the **transfer of personal data to AWS in Japan is also permissible**.

Trend Micro provides a **list of processors and sub-processors** by product or service, which will be updated on a regular basis, and lists all Trend Micro affiliates and third-party sub-processors, which are authorized to process customer data: https://www.trendmicro.com/en_us/about/legal/subprocessors.html.

4. Lawfulness of Data Processing by Means of Trend Micro Customer Support

a) Processing is necessary for the performance of a contract (Art. 6(1)(b) GDPR)

Personal data that is necessary for the performance of the contract for Trend Micro Customer Support, entered into with the customer, such as the PSP Agreement, includes the customer data explained above in Chapter II 2). This data will be collected and processed by Trend Micro for providing and invoicing the Trend Micro Customer Support to the customer, and thus its **processing is necessary for the performance of the Trend Micro Customer Support contract vis-à-vis the customer** pursuant to Art. 6(1)(b) GDPR.

b) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Art. 6(1)(f) GDPR)

Trend Micro Customer Support will not only be provided to support customers with technical product issues, but also *inter alia* for security assessments, proactive antivirus support, advanced malware incident assistance, **threat/malware analysis, threat hunting,** and **managed detection and response services**. As explained in Chapter II 5) above, in this context, Trend Micro might access personal data of individuals contained in files, such as dump files or emails, examined by Trend Micro Customer Support or data collected by Managed XDR.

Trend Micro Customer Support and Managed XDR experts help customers in **ensuring their network and information security**. Meaning, the ability of a network or an information system to resist–at a given level of confidence–accidental events, unlawful, or malicious actions that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal data, as well as the security of the related services offered by, or accessible via those networks and systems. An example of this would be **preventing unauthorized access to electronic communication networks** and **malicious code distribution**, as well as stopping 'denial of service' attacks and damage to computer and electronic communication systems.

The collecting, processing, and sharing of personal data, when providing Trend Micro Customer Support as laid down above, is **necessary for the purposes of those legitimate interests pursued by the customer (for ensuring its network and information security) and Trend Micro (for providing, improving, and optimizing its products and services)**. Personal data collected and processed by Trend Micro, in the course of the provision of Customer Support, will be utilized by Trend Micro products to identify and isolate threats, vulnerabilities, suspicious activities, and attacks, as well as analyze emails and protect against suspicious or malicious content. The information will also be used by Trend Micro to enhance virus protection, intrusion detection, prevention and protection, network defense, and the dispatch of product updates. By doing this, **legitimate interests of third parties are also pursued**, namely of other users of Trend Micro products and services and the internet community in general. This is because the threat and malware analysis by Trend Micro Customer Support results in a permanent updating of information about detected threats and malware throughout the internet and not only with respect to each individual customer. This allows Trend Micro customers to rapidly identify and defend against potential threats within their own unique network environment, as well as enabling Trend Micro to provide Customer Support to its customers.

According to recital 49 of the GDPR, the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by providers of electronic communications networks and services and by providers of security technologies and services constitutes a legitimate interest of the data controller concerned, i.e. the customer. This requirement will be fulfilled by Trend Micro Customer Support, since it avoids identifying persons as much

as possible. For example, Trend Micro Customer Support refrains from collecting a large amount of personal data, anonymization or pseudonymization, creating non-reversible file hashes, and only sharing metadata and meta information of detected malware wherever possible. In terms of customer's endpoint IP addresses, only in exceptional circumstances can a person be identifiable by means of endpoint IP addresses. No emails or files, other than those which are suspicious or malicious, will ever be stored by Trend Micro. For those that are stored, they will be anonymized or pseudonymized where applicable, and after examination, the emails and files will be deleted from the Trend Micro systems.

These legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data. In terms of customers' employees, whose data will be collected through Trend Micro Customer Support, the **customer can minimize personal data of the employees** involved. Customers can do this by avoiding the inclusion of personal data, such as someone's name on a file path, host name, or computer name on files being sent to Trend Micro for threat/malware analysis. Access to personal data by Trend Micro employees, in relation to Customer Support, is limited to what is necessary, and when handling cases, usually no individuals can be identified unless suspicious emails contain respective information. For all of its products, Trend Micro provides a **data collection disclosure** on what kind of data a Trend Micro product collects and how the customer can **opt-out of the data collection**.

In addition, it is also in the legitimate interest of the employees of Trend Micros' customers to be protected against attacks and malicious emails, websites, and files. In regards to **external parties** communicating with the customer organization, they must anticipate that their correspondence will be examined, whether it contains malicious data or if they attack the customer's organization, and thus have **no overriding interest**. The same holds true for websites accessed by the customer. Attackers going after the network or information systems of the customer or cybercriminals sending spam, suspicious, or malicious content have no prevailing interest in the protection of their personal data.

Summed up, the collection and processing of personal data by Trend Micro Customer Support can be considered as being necessary for the purposes of the legitimate interests pursued by the controller (the customer) and by third parties, in particular, other users of Trend Micro products and the internet community in general, and thus lawful pursuant to Art. 6(1)(f) GDPR.

5. Trend Micro Adheres to the Principles of Art. 5 GDPR

a) Lawfulness, fairness, and transparency

As just explained under no. 4 above, the processing of personal data, when providing Trend Micro Customer Support, is **lawful** and **fair**. Trend Micro also is **transparent** about its data

processing, in particular, by means of its **privacy notice** (see https://www.trendmicro.com/en_us/about/legal/privacy.html) and its data collection disclosure (see https://success.trendmicro.com/data-collection-disclosure).

b) Purpose limitation

When providing Trend Micro Customer Support, Trend Micro only collects personal data for specified, explicit, and legitimate purposes, as explained in detail above. Trend Micro does not process such personal data in a manner that is incompatible with those purposes.

c) Data minimization

Trend Micro adheres to the **principle of data minimization** when providing Trend Micro Customer Support, since it avoids identifying persons as much as possible, for example, by refraining from collecting a large amount of personal data, anonymization or pseudonymization, creating non-reversible file hashes, and only sharing metadata and meta information of detected malware, wherever possible. In terms of customer's endpoint IP addresses, only in exceptional circumstances can a person be identifiable by means of endpoint IP addresses. No emails or files, other than those which are suspicious or malicious, will ever be stored by Trend Micro. For those that are stored, they will be anonymized or pseudonymized where applicable, and after examination, the emails and files will be deleted from the Trend Micro systems.

d) Accuracy

Trend Micro ensures that the personal data collected and processed is **accurate,** and where necessary, **kept up to date**. If it turns out that that such personal data is inaccurate, in regard to the purposes for which it was processed, it will be erased or rectified without delay.

e) Storage limitation

Trend Micro adheres to the **principle of storage limitation** and has established **general data retention policies**. Some of the measures that have been implemented on Trend Micro's CRM to ensure customers' personal data are not held for longer than is required are as follows:

- CRM contacts details. Typically, the contact record contains the following personal data: Salutation, first name, last name, job function, work address, work email, and work phone number. Additional contact details, such as mobile phone, fax number, or remote session ID, can be provided if the customer wants to be contacted through these communications channels as well. These contact records are removed after two years of no interaction with Trend Micro.

- CRM case details. These records are deleted five years after case closure. This provides sufficient case history to support customers with a macro view of any issues they have had during their Trend Micro product life cycle.
- Log files collected. These files are deleted one year after case closure.
- Dump files. Dump files, which customers may need to send in for threat/malware analysis, will be archived after 90 days and deleted in nine months.

f) Integrity and confidentiality

Trend Micro has implemented **TOM** pursuant to Article 32 GDPR and has taken **additional security measures** to protect personal data, which include:

- Global Information Security Policy. Trend Micro has enacted a Global Information Security Policy, which includes *inter alia* the Technical and Organizational Measures and the Software Security Policy, and applies to the whole Trend Micro organization, including the Trend Micro support teams, which operate worldwide.
- Security. Trend Micro has implemented the relevant TOM required to safegaurd all personal data stored and ensure the ongoing confidentiality, integrity, availability, and resilience of Trend Micro's processing systems and services. The TOM includes access control, transmission control, input control, job control, availability control, network control, endpoint control, and incident and log management. They form an annex to the Trend Micro Data Processing Addendum and can be retrieved here: https://www.trendmicro.com/en_us/about/legal/data-processing-addendum.html.
- Two-factor authentication. Trend Micro provides two-factor authentication on various websites, where customers provide personal data to Trend Micro.
- Anonymization and pseudonymization. Trend Micro will anonymize or pseudonymize personal data where applicable.
- Data encryption and access control. Trend Micro's software allows customers, as well as Trend Micro service operation teams, to protect data through logical access controls (e.g. authentication controls like passwords and authorization controls), encryption in transit (inter alia TLS 1.2+), and encryption at rest (e.g. hashing passwords and other sensitive data).
- High software security standards. All Trend Micro developers, including the CSEs, are bound to Trend Micro's Software Security Policy. This policy provides detailed requirements for a software security committee, vulnerability management, integration of security practices when designing new features, performance of security assessments of web applications, protection of personal and sensitive data, a secure product pipeline, separate development and test environments from production, and software security training.
- Certifications. Trend Micro's software and services adheres to the standards, with widely recognized certifications, such as ISO 27001 and PCI DSS.
- Training. Trend Micro has provided training and enablement programs for its employees to ensure a strong awareness of the GDPR and its requirements.

- Data ownership. Trend Micro acknowledges the data ownership of the customer and allows customers to retrieve or delete their personal data, if needed.
- Rights of the individual. Trend Micro has the necessary mechanisms in place that allow individuals to exercise their rights under the GDPR. This includes their right to erase and right of access to their data. For further information, please see the Trend Micro privacy notice: https://www.trendmicro.com/en_us/about/legal/privacy.html.

All **Trend Micro employees** who provide Customer Support, regardless of where they are located, have to comply with the Trend Micro Global Information Security Policy and have **committed themselves to confidentiality and data protection**.

Access to personal data by Trend Micro employees, in relation to Customer Support, is limited to what is necessary, and when handling cases, usually no individuals can be identified unless suspicious emails contain respective information.

g) Data Protection Officer and GDPR support team

Trend Micro has appointed a **data protection officer for Europe** and a **GDPR support team** to ensure that its privacy processes and procedures continue to be consistent with data protection regulations, including the GDRP.

h) Data protection by design and by default

Trend Micro is committed to data protection by design and by default as the core of all current and future initiatives. Focusing on **security by design**: All Trend Micro developers are bound to **Trend Micro's Software Security Policy,** which provides detailed requirements *inter alia* for the integration of security practices when designing new features and the protection of personal and sensitive data. For all of its products, Trend Micro provides a **data collection disclosure** on what kind of data a Trend Micro product collects and how the customer can **opt-out of the data collection**.

Status: 30 July 2020