Data Protection Policy v1.1
Trend Micro Europe
## Table of Contents

1. **Introduction** ................................................................................................................................. 3
2. **Glossary** ........................................................................................................................................ 3
3. **Scope & Purpose** ............................................................................................................................. 4
4. **Policy Responsibility** ...................................................................................................................... 4
5. **Data Protection Principles** ............................................................................................................... 5
   5.1 Lawful, Fair & Transparent .................................................................................................................... 5
   5.2 Purpose Limitation ............................................................................................................................ 6
   5.3 Data Minimisation ............................................................................................................................ 6
   5.4 Accuracy .......................................................................................................................................... 7
   5.5 Storage Limitation ............................................................................................................................ 7
   5.6 Integrity, Confidentiality & Security ................................................................................................. 7
   5.7 Accountability for demonstrating compliance .................................................................................. 9
6. **Rights of Individuals whose data is collected** .................................................................................. 10
   6.1 Right of Access by the Data Subject ................................................................................................. 10
   6.2 Right to Rectification ....................................................................................................................... 10
   6.3 Right to Erasure (right to be forgotten) ............................................................................................ 10
   6.4 Right to Restriction of Processing .................................................................................................... 11
   6.5 Right to Data Portability .................................................................................................................. 11
   6.6 Right to Object .................................................................................................................................. 12
   6.7 Right not to be subject to Automated Decision Making ....................................................................... 12
   6.8 Right to Complain ............................................................................................................................ 12
7. **Responsibilities of Trend Micro** ....................................................................................................... 13
   7.1 Ensuring appropriate technical and organisational measures ......................................................... 13
   7.2 Data protection by design and by default .......................................................................................... 13
   7.3 Implementing appropriate agreements with third parties ................................................................. 13
All such agreements shall be implemented in accordance with article 28 in writing prior to the commencement of the transfer of personal data. .................................................................13

7.4 Transfers of personal data outside of the European Economic Area ................................13

7.5 Maintaining an inventory of data processing .................................................................13

7.6 Personal data breaches .................................................................................................14

7.7 Data protection impact assessments (DPIA). ...............................................................14

8. The Data Protection Officer’s Responsibilities .................................................................14

8.1 Appointment of a DPO .................................................................................................14

8.2 Management Facilitation of the DPO ..........................................................................15

8.3 Responsibilities of the DPO .........................................................................................15

8.4 Data Protection Impact Assessments ............................................................................16

9. Responsibilities of Staff and Similar Parties .................................................................17

1.1 Training .........................................................................................................................17

1.2 Consequences of failing to comply ................................................................................17

10. Procedure Audits ........................................................................................................18

11. Data Protection Queries ...............................................................................................18

12. Approvals and sign offs ...............................................................................................19

13. Version control .............................................................................................................19
1. Introduction

This document outlines Trend Micro Data Protections policies for Europe.

2. Glossary

The following table identifies some of the terms referred to within this policy.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Controller</td>
<td>Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;</td>
</tr>
<tr>
<td>Data Custodian</td>
<td>The IT department personnel responsible for managing the technical controls used to secure data within an organisation are referred to as custodians of the data.</td>
</tr>
<tr>
<td>Data End-user</td>
<td>The person who actually obtains, processes or uses the data on a day to day basis is called the data end-user.</td>
</tr>
<tr>
<td>Data Owner</td>
<td>A data owner is a delegated person at management level in an Organisation responsible for the management and security of data.</td>
</tr>
<tr>
<td>Data Processor</td>
<td>Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>A Trend Micro appointed officer with responsibility for the Data Protection compliance of the organisation.</td>
</tr>
<tr>
<td>Data Subject</td>
<td>A data subject is an individual who is the subject of personal data which is held by a data controller or processed by a data processor.</td>
</tr>
<tr>
<td>GDPR</td>
<td>The new EU General Data Protection Regulation (GDPR) - Regulation 2016/679 which comes into effect in May 2018 and replaces the current Data Protection Directive 95/46/EC .</td>
</tr>
<tr>
<td>Personal Data</td>
<td>'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;</td>
</tr>
<tr>
<td>Processing</td>
<td>Processing 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;</td>
</tr>
<tr>
<td>Sensitive Personal Data</td>
<td>Any personal data relating to a person’s racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.</td>
</tr>
</tbody>
</table>
3. Scope & Purpose

This policy applies to all of Trend Micro functions which process personal data in relation to identified or identifiable natural persons, including the processing performed on customers', clients', employees', suppliers' and any other personal data Trend Micro processes from any source.

Under Article 4 of the GDPR:

- **Personal data** is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Special categories of personal data** is defined as any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The purpose of this Data Protection Policy is to enable Trend Micro to:

- Ensure compliance with EU and Member State data protection legislation
- Outline best practice in relation to the processing of data
- Protect the organisation, clients, staff and any other individuals from the consequences of a data breach

The GDPR confers rights on individuals as well as responsibilities on those persons processing personal data. This policy sets out how Trend Micro seeks to process personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

Trend Micro may supplement or amend this policy with additional policies and guidelines from time to time.

4. Policy Responsibility

The Board of Trend Micro have overall responsibility for ensuring that the organisation is committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information Trend Micro collects and processes.
The Data Protection Officer, Department and Function Managers are responsible for ensuring that this policy is implemented across the organisation. Managers at all levels of Trend Micro will be accountable for being able to demonstrate that this policy has been implemented across their respective divisions and are responsible for ensuring that their staff observe its provisions.

5. Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles set out under Article 5 of the GDPR. Trend Micro policies and procedures should be designed to ensure compliance with the following principles:

5.1 Lawful, Fair & Transparent

- **Lawful** – Trend Micro is required to identify and document the lawful basis for processing personal data. legitimate interest, the provision of consent by the data subject; legal obligation, the performance of a contract to which the data subject is party (or in order to take steps at the request of the data subject prior to entering a contract); the protection of the vital interests of the data subject; or for the performance of a task carried out in public interest.

- **Fair** – in order to process personal data fairly, Trend Micro is required to make certain information available to the data subject. This is applicable whether the personal data has been obtained directly from the data subjects or obtained from another source, including:
  - Trend Micro contact details (where Trend Micro determines they are not the data controller, the contact details of the data controller will need to be provided)
  - Trend Micro Data Protection Officer (DPO) details (If applicable, the controller’s DPO contact details must be provided)
  - A complete and transparent list of the purposes of processing, and the legal basis for all processing carried out by Trend Micro
  - Retention periods for each category of data
  - A list of the rights of the data subject as outlined under GDPR
  - A list of recipients/categories of recipients of the personal data
  - A list of transfers of personal data to third countries

- **Transparent** – Trend Micro will provide the information outlined above to the data subject at the time personal data is collected. Trend Micro will ensure that the information provided is detailed and specific, and that such notices are understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. In order to balance the requirements above, Trend Micro may implement appropriate policies to make information available on its website. The information provided must include information about personal data collected directly from the data subject and personal data collect from other sources.

In line with the publication of a privacy notice:
• Trend Micro staff, will be made aware of the information held relating to them upon request and of what information can be disclosed and guidelines on this will be included in staff induction and staff manuals;
• Trend Micro staff and job applicants will be made aware of the personal information held and its purpose of processing;
• Trend Micro staff and clients will be made aware of the CCTV information held and its purpose;
• Trend Micro clients will be made aware that data can be exchanged with third parties;
• Trend Micro clients will be made aware that they can request to have their details removed by emailing Trend Micro Data Protection Officer.

Trend Micro aims to demonstrate the lawful, fair and transparent processing of personal data the implementation of the following practical measures:

• Developing a Privacy Notice outlining the rights of the data subject as well as details of the processing being carried out by Trend Micro using their personal data (as outlined above). This notice will be publicly available on Trend Micro website and issued to the data subject on receipt of new personal data;

5.2 Purpose Limitation
- Personal data can only be collected for specific, explicit and legitimate purposes

Trend Micro will collect and process personal data only for the purposes for which it is collected. Trend Micro staff must be alert to requests for processing of personal data for purposes for which it was not collected, no matter how related the processing may appear. Processing should only continue after an assessment of the impact of the new processing.

Trend Micro aims to demonstrate the limitation of the purpose of processing personal data through the implementation of the following practical measures:

• Ensuring data processing is carried out for the purposes specified or as justified and documented under another lawful basis as set out in the Trend Micro Privacy Policy;
• Ensure that disclosures of information will be carried out for the purposes specified under or as justified and documented under other applicable legislation;
• Ensuring that all Trend Micro staff and clients are made aware that transfers of personal data to third parties and public bodies are performed in accordance with statutory or legal obligations.

5.3 Data Minimisation
- Personal data must be adequate, relevant and limited to what is necessary for processing

Trend Micro will ensure that in designing methods of data collection, whether online forms, hardcopy, or other means, that only the personal data required to identify the data subject and provide the benefit or service requested will be processed. Trend Micro will undertake regular reviews of the data requested to ensure that the amount of personal data collected is minimised.

Trend Micro aims to demonstrate the minimisation of personal data through the undertaking of regular reviews of the data requests to ensure the volume of personal data collected is minimal.
5.4 Accuracy

- **Personal data must be accurate and kept up to date with every effort to erase or rectify without delay**

All data subjects have a right to ensure that their data is accurate and complete. Trend Micro requires accurate and up-to-date data regarding the data subject in order to ensure that the correct benefits and services are provided to the correct recipients. All data collection procedures should be designed to ensure that reasonable steps are taken to update personal data where new data has been provided. All changes to personal data should be shared with each third party with whom the previous data had been shared, unless this is impossible or requires disproportionate effort.

Trend Micro aims to demonstrate commitment to the maintenance of accurate personal data through the implementation of the following practical measures:

- The encouragement of accurate data entry through system design and Trend Micro staff training;
- The prevention of duplication of storage of personal data where possible;

5.5 Storage Limitation

- **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing**

Trend Micro will implement appropriate policies and procedures to ensure that personal data is retained only for the minimum period required to provide the benefit or services requested by the data subject. This may be achieved by destroying or anonymising the personal data, or by any other appropriate method.

Trend Micro aims to demonstrate the limitation of personal data stored through the implementation of the following practical measures:

- The development of an Trend Micro Data Retention and Disposal Schedule which will apply to data in all formats (including hardcopy, electronic, information held on Trend Micro portable devices, the use of CCTV footage);
- The scheduled developed will be subject to a number of legislative provisions and will be considered when formulating the records Retention and Disposal Schedule (i.e. Equality Legislation, Working Time Act, Employment Acts, Finance Acts);

5.6 Integrity, Confidentiality & Security

- **Personal data must be processed in a manner that ensures appropriate security**

Trend Micro will implement appropriate technical and organisation measures to ensure that appropriate security of the processing of personal data is implemented, including:

Information Security Policies and Organization
Trend Micro will maintain an information security program which adopts and enforces internal policies and procedures, designed to (a) satisfy security objectives, (b) identify reasonably foreseeable and internal risks to security, and (c) minimize security risks. Trend Micro will designate personnel to coordinate the information security program.

Access Control to Processing Areas

Trend Micro implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are processed or used. Physical controls are implemented to prevent unauthorized entrance to facilities where physical components are housed (the “Facilities”), including electronic or human security personnel controls.

Trend Micro provides access to facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges, the access privileges are revoked.

Trend Micro implements monitoring measures at access points, and ensures that all physical access to the Facilities by employees and contractors is logged and routinely audited.

Access Control to Data Processing Systems

Trend Micro implements suitable measures to prevent its data processing systems from being used by unauthorized persons. Trend Micro will maintain access controls and policies to manage what access is allowed to each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Trend Micro will maintain corrective action and incident response plans to respond to potential security threats.

Access Control to Use Specific Areas of Data Processing Systems

Trend Micro commits that the persons entitled to use its data processing system are only able to access the data within the scope and to the extent covered by its access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization.

Transmission Control

Trend Micro implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media, including the use of firewalls or functionally equivalent technology to protect personal data.

Input Control

Trend Micro implements suitable measures to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems or removed.

Job Control

Trend Micro ensures that personal data may only be processed in accordance with written instructions issued by exporter.
Trend Micro ensures that if security measures are adopted through external entities it obtains written description of the activities performed that guarantees compliance of the measures adopted with this document. Trend Micro further implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received.

Availability Control

Trend Micro implements suitable measures to ensure that personal data are protected from accidental destruction or loss.

Separation of processing for different purposes

Trend Micro implements suitable measures to ensure that data collected for different purposes can be processed separately.

Trend Micro system administrators (if any):

Trend Micro implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This is accomplished by:

Continued Evaluation

Trend Micro will conduct periodic reviews of the security of its network and infrastructure as well as adequacy of its information security program according to industry security standards and its policies and procedures. Trend Micro will continually evaluate the security of its network and Infrastructure and associated Services to determine whether additional security measures are required to respond to new risks or findings generated as a result of the periodic reviews.

5.7 Accountability for demonstrating compliance

Trend Micro will ensure that an adequate record of the processing of personal data is maintained and that Trend Micro can evidence that it has complied with this policy and related policies and procedures. Responsibility for collecting and maintaining the evidence is with Management [insert more specific role/title if applicable]. Refer to section 3 of this policy for further guidance.
6. Rights of Individuals whose data is collected

Trend Micro will design and maintain appropriate policies, procedures and staff training to ensure the fulfilment of the following data rights of data subjects.

6.1 Right of Access by the Data Subject

Article 15, GDPR

The data subject has the right to access of the personal data which is being processed by Trend Micro in relation to them.

Trend Micro will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled within 30 days of receipt as required under the GDPR.

Please refer to the [Trend Micro Data Access Request] process for further details.

6.2 Right to Rectification

Article 16, GDPR

The data subject has the right to request the rectification of the personal data being processed by Trend Micro in relation to them if the data is deemed to be inaccurate or incomplete.

Trend Micro will implement appropriate controls to ensure that personal data held is accurate and as up to date as reasonably possible as well as procedures for the rectification of personal data on receipt of a valid request for rectification.

Trend Micro will issue letters to the data subject confirming the receipt of the request and updating the data subject on the outcome of the request thereafter.

On completion of a request for rectification, Trend Micro will notify all recipients of the data impacted. Additionally, Trend Micro will inform the data subject of all third parties notified upon request.

6.3 Right to Erasure (right to be forgotten)

Article 17, GDPR

The data subject has the right to seek the erasure of their personal data by Trend Micro if:

- The personal data is no longer required for the purposes for which it was obtained by Trend Micro
- The data subject withdraws consent for data which is being processed by Trend Micro on the basis of consent
- The personal data is being unlawfully processed by Trend Micro
- The data subject has a valid objection to the processing of their personal data by Trend Micro
- The personal data requires deletion in line with legal requirements.

Trend Micro will not be required to fulfil an erasure request if the associated processing activity is necessary for:

- Exercising the right of freedom of expression and information
• Compliance with legal obligation or for the performance of a task carried out in public interest
• Reasons of public interest in the area of public health
• Archiving or statistical purposes in the public interest
• The establishment, exercise or defence of legal claims.

On receipt of a valid request for erasure from the data subject, Trend Micro will carry out an assessment of the justification for the retention of the personal data in question. Trend Micro will implement appropriate procedures to carry out this assessment and will document the justification for the retention of all personal data for issue to the data subject on receipt of a request for erasure that does not require fulfilment.

Trend Micro will issue letters to the data subject confirming the receipt of the request and updating the data subject on the outcome of the request thereafter.

On receipt of a request for erasure, Trend Micro will notify all recipients of the data impacted. Additionally, Trend Micro will inform the data subject of all third parties upon request.

6.4 Right to Restriction of Processing
Article 18, GDPR

The data subject has the right to restrict the extent of processing of personal data on receipt of a valid request if:
• The accuracy of the personal data is contested by the data subject
• The processing of the personal data is unlawful and the data subject opposes the erasure of the data
• The personal data is no longer required by the data controller, but retention is required by the data subject
• The data subject has a pending objection to the processing of the personal data.

Trend Micro will implement and maintain appropriate procedures to assess whether a data subject request to restrict the processing of personal data can be implemented. Trend Micro will issue letters to the data subject confirming the receipt of the request and where the request for is fulfilled, Trend Micro will write to the data subject to confirm the restriction has been implemented and when the restriction is lifted.

6.5 Right to Data Portability
Article 20, GDPR

The data subject has the right to the provision of all of the personal data held in relation to them to the data subject or to a specified third party in a structured, commonly used and machine-readable format where:
• Processing is completed on the basis a contract
• Processing is completed based on the provision of consent by the data subject
• Processing is carried out by automated means.

Trend Micro will implement appropriate procedures to compile and transfer the relevant personal data in the required format.

Trend Micro will issue letters to the data subject confirming the receipt of the request and updating the data subject on the outcome of the request thereafter.
6.6 **Right to Object**  
*Article 21, GDPR*

The data subject has the right to object to the processing of his or her personal data. The processing must have been undertaken on the basis of public interest or legitimate interest by Trend Micro.

Trend Micro will implement and maintain procedures to allow data subjects to pursue their right to object.

Trend Micro will issue letters to the data subject confirming the receipt of the objection and updating the data subject on the outcome of the objection thereafter.

6.7 **Right not to be subject to Automated Decision Making**  
*Article 22, GDPR*

The data subject has the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning him or her.

Trend Micro is not currently carrying out any fully automated decision making using personal data. Trend Micro will ensure that if systems or processes are implemented that calculate benefits or services then an appropriate right of appeal to a member or panel of Trend Micro staff is available to the data subject.

6.8 **Right to Complain**

Trend Micro will implement and maintain a complaints process whereby the data subject will be able to contact the Data Protection Officer. The Data Protection Officer will work with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject will be informed of their right to bring their complaint to the Office of the Data Protection Commissioner and will be provided with the appropriate contact details.
7. Responsibilities of Trend Micro

Trend Micro has responsibility for the following:

7.1 **Ensuring appropriate technical and organisational measures**

Trend Micro will implement appropriate technical and organisational measures to ensure and be able to evidence that it is always protecting personal data.

Including:
- Pseudonymising and encrypting personal data
- Ensuring ongoing confidentiality, integrity, availability and resilience of processing
- The ability to restore the availability and access to personal data in a timely manner in the event of an incident
- Regular testing, assessing and evaluating of the effectiveness of the organisational and technical measures in place.

7.2 **Data protection by design and by default**

Data controllers must, at the time of determining the means of processing as well as while completing the processing, implement appropriate technical and organisational measures to implement the data protection principles set out in article 5 of the GDPR (listed above) and integrate necessary safeguards into the processing to meet GDPR requirements.

7.3 **Implementing appropriate agreements with third parties**

Trend Micro will implement appropriate agreements, memoranda of understanding, bilateral agreements and contracts (collectively “agreements”) with all third parties with whom personal data is shared.

All such agreements shall be implemented in accordance with article 28 in writing prior to the commencement of the transfer of personal data.

7.4 **Transfers of personal data outside of the European Economic Area**

Trend Micro will ensure that the transfer of personal data of the data subject outside of the European Economic Area is done so using the mechanism of model clauses in place to ensure an adequate level of protection in place.

7.5 **Maintaining an inventory of data processing**

Trend Micro will maintain an inventory of the processing activities completed using personal data in the manner prescribed by article 30 of the GDPR. The inventory will be reviewed and signed off by Senior Management, not less than on annual basis and will be made available to the Supervisory Authority on request.
7.6 **Personal data breaches**

Trend Micro defines a ‘personal data breach’ as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (for example, the most common breach incidents that can occur are correspondence issuing to an unauthorised third party). Trend Micro deems any loss of personal data in paper or digital format to be a data breach.

Trend Micro will develop and maintain a procedure for handling Data Breaches. This procedure will establish the methodology for handling a personal data breach and for the notification of the breach to the Office of the Data Protection Commissioner and to data subject where it is deemed necessary.

7.7 **Data protection impact assessments (DPIA)**

Trend Micro will implement procedures and documentation whereby all types of processing, in particular the use of new technologies, that result in a high risk to the rights and freedoms of the data subject shall carry out a data protection impact assessment. As part of this process, a copy of the impact assessment shall be shared with Trend Micro Data Protection Officer.

Where Trend Micro is unable to identify measures that mitigate the high risks identified through completion of the DPIA, Trend Micro will consult with the Office of the Data Protection Commissioner prior to the commencement of processing.

8. **The Data Protection Officer’s Responsibilities**

Under the GDPR, it is recommended for Trend Micro to formally appoint a Data Protection Officer (DPO). The DPO’s role will facilitate data protection compliance and ensure that Trend Micro is carrying out its ‘core activities’ – primary services – of processing personal data in accordance with the protections afforded to the data subject under EU and Member State data protection legislation.

The published details must include a postal address, a dedicated telephone number, and a dedicated e-mail address.

The DPO must be included in any matters involving data protection at the earliest possible stage, including privacy impact assessments, data processing activities which may affect the data subject, and incidents which effect the personal data of the data subject. This may involve the DPO attending middle and senior management meetings. Where it is decided not to follow the DPO’s advice, the matter of discussion, the discussion, the DPO recommendation, and the reasons for not adhering to the recommendation should be formally recorded.

8.1 **Appointment of a DPO**

Under Article 37(5) of the GDPR, the DPO “shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39”.

Furthermore, the DPO role cannot be assigned to someone where their other role(s) and their DPO duties present a conflict of interest.
8.2 *Management Facilitation of the DPO*

Under Article 38(2) of the GDPR, Trend Micro management must also support the DPO by providing:

- The necessary resources to carry out his/her tasks, including finance, infrastructure (premises, facilities, and equipment), and staff where appropriate;
- Access to personal data and processing operations;
- The resources for him/her to maintain their expert data protection knowledge such as continuous training;
- Active support by senior management;
- Adequate time to fulfil their DPO duties. Best practice would be to dedicate a percentage of their weekly time to data protection activities;
- Communication of the DPO role and their activities to employees within Trend Micro;
- Access to other services such as, but not limited to, HR, legal, IT, and security for support and information to fulfil their duties.

The DPO must also not receive any instructions regarding the exercise of his / her tasks, and must be in a position to perform his/her duties and tasks in an independent manner. The DPO cannot “be dismissed or penalised by the controller (Trend Micro) or the processor for performing his / her tasks”.

8.3 *Responsibilities of the DPO*

The DPO will report to Trend Micro Board concerning the tasks allocated to them. The responsibilities of the Data Protection Officer will include the following:

i. Keeping the Management Board, Trend Micro staff, and other stakeholders updated on data protection responsibilities, risks and issues;
ii. Monitoring compliance with EU Regulations on data protection, ePrivacy and European Data Protection Laws and Regulations;
iii. Monitoring that all data protection policies and policies are reviewed and updated on a regular basis;
iv. Monitoring that Trend Micro provides appropriate data protection training and advice for all staff members and those included in this policy;
v. Providing advice where requested as regards the data protection impact assessments and monitoring that such assessments are completed to an appropriate standard;
vi. Responding to individuals such as clients and employees who wish to know which data is being held on them by Trend Micro;
vii. Monitoring that appropriate data processing agreements are put in place with third parties that handle Trend Micro’s data and ensuring that reviews on third party data protection compliance are carried out on a regular basis;
viii. Monitoring that a data inventory data audit to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant;
ix. Acting as a point of contact and cooperating with the Office of the Data Protection Commissioner.
8.4 Data Protection Impact Assessments

It is the task of Trend Micro, not the DPO, to carry out Data Protection Impact Assessments (DPIA’s) as necessary. However, the DPO should provide advice and guidance at each stage of the DPIA including:

- Whether or not to carry out a DPIA;
- What methodology to follow when carrying out a DPIA;
- Whether to carry out the DPIA in-house or whether to outsource it;
- What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;
- Whether or not the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

Again, where adherence is not paid to the DPO’s advice, this should be formally recorded using the DPIA documentation.

Further information can be obtained from Guidelines on Data Protection Officers (’DPOs’) Article 29 WP.
9. Responsibilities of Staff and Similar Parties

Anyone who processes personal data on behalf of Trend Micro has a responsibility to comply with this data protection policy and ensure compliance with the principles of data protection. All records created in the course of carrying out their duties are the property of Trend Micro and subject to its overall control.

Anyone who processes Trend Micro data is required to:

- Read, understand and accept any data protection policies, procedures and guidelines drawn up by Trend Micro
- Ensure that all data they access, manage and control as part of their daily duties is carried out in accordance with data protection requirements
- Return all Trend Micro data held upon termination of their contract of employment, retiring or changing position within Trend Micro
- Ensure data protection compliance within their division.

1.1 Training

All Trend Micro staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided as required or whenever there is a substantial change in the law or our policy and procedure.

Training is mandatory for all Trend Micro staff and will cover:

- The General Data Protection Regulation relating to data protection
- Our data protection and related policies and procedures.

1.2 Consequences of failing to comply

All current and former employees of Trend Micro may be held accountable in relation to data processed, managed and controlled by them during the performance of their duties in the organisation.

Individuals found to be in breach of Trend Micro data protection policies may be subject to Trend Micro disciplinary procedures. If staff consider that this policy has not been followed, they should raise the matter through their line manager and with the Data Protection Officer.
10. **Procedure Audits**

Trend Micro InfoSec Team with the assistance of Internal Audit will provide oversight of data protection as part of its work programme including the review of the storage, handling and protection of personal data.

The particular focus of any review by Internal Auditors will be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any breach of data protection regulations.

Risks associated with the storage, handling and protection of personal data are to be included in Trend Micro’s risk register and risk assessments should take place as part of a Department’s risk strategy exercise.

Furthermore, external audits of all aspects of Data Protection within the organisation may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

11. **Data Protection Queries**

Trend Micro has resources on its internet site and you should refer to these in the first instance.

If you cannot find the answer to your query on the website then do not hesitate to contact our Data Protection Officer,

Lianne Harcup  
C/o Trend Micro Emea limited  
Median House  
Ida Business Park  
Model Farm Road  
Cork  
Ireland  
TEL: +353-21-730 7300  
Email: GDPR@Trendmicro.com
12. Approvals and sign offs

This policy comes into effect on 25 May 2018.

<table>
<thead>
<tr>
<th>Document Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Owner(s)</td>
</tr>
<tr>
<td>Date approved</td>
</tr>
<tr>
<td>Approved by</td>
</tr>
<tr>
<td>Next review date</td>
</tr>
</tbody>
</table>

The next review of this policy is scheduled for May 2019. The Trend Micro GDPR Team is responsible for initiating the review.

13. Version control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes made by</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>23/05/2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>26/11/2019</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>