DATA PROTECTION POLICY

TPV Technology Limited

1 January 2018

DATA PROTECTION POLICY (the "Policy")

I. INTRODUCTION

Data Protection is an important consideration in the workplace and when conducting a business. A number of individuals in the organisation may have access to personal data relating to Staff (this term shall apply to all employees, to Directors and to those who work for TPV in any other capacity, including agency workers and any other person who works under a contract in terms of which he/she has agreed personally to provide services to TPV; Staff will include retired employees, temps, terminated employees, consultants, trainees, secondees, contractors, students, volunteers, *etc*.) and/or clients, customers, consumers and users of TPV's products, suppliers and other individuals during the course of their work with TPV.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the Dutch Data Protection Act of 1 September 2011, as amended from time to time, in particular per 1 January 2016 with amendments regarding of fines and data breaches have placed obligations on TPV with regard to how it processes personal data and has created rights for people whose personal data are processed. On April 27, 2016,new legislation was adopted by the EU by means of the General Data Protection Regulation (OJ L 119, 4.5.2016, p. 1–88), which will take effect from 25 May 2018 (hereinafter referred to as "GDPR"). All the applicable laws together are hereafter called "Data Protection Legislation".

This Policy provides an overview of the current and expected general data protection law requirements TPV and its Staff must comply with when processing personal data.

Compliance with this Policy is essential for the following reasons:

- compliance with data protection law is a legal obligation: failure to abide by those laws can lead to the imposition of fines, claims for damages and even criminal sanctions;
- compliance with data protection law will establish a trust relationship between TPV and its business partners as well as its Staff;
- compliance with data protection law leads to efficiency gains by creating and retaining value in databases and systems used.

II. SCOPE OF APPLICATION

1. This Policy is applicable to all TPV operations, such as TP Vision, MMD and AOC in Europe and is subject to the General Data Protection Regulation (EU 2016/679) and any other (still) applicable laws, directives and regulations.

2. This Policy is subject to any global Data Privacy Policy, which policy will leading in case of internal contradictions. The Policy is further subject to TPV's current and related policies.

3. This Policy applies as a corporate guideline to TPV and all of its employees and contractors, who may, in the scope of their job duties, process personal data wholly or partly by automatic means or perform any other processing (otherwise than by automatic means) of personal data which form part of a filing system or are intended to form part of a filing systems.

4. This Policy is designed to provide a uniform minimum standard for the protection of personal data throughout the TPV organisation. It shall be applied without prejudice to the applicable Data Protection Legislation which may impose stricter obligations and requirements.

III. DATA PROTECTION OFFICER (THE "DPO")

1. TPV shall appoint a privacy contact person (hereinafter the "**DPO**").

2. The DPO, whois independent with respect to execution of its data privacy related responsibilities and in this respect not bound by internal line management instructions, shall supervise TPV's compliance with Data Protection Legislation and this Policy.

IV. PRIVACY TEAM

1. TPV shall appoint a privacy team (hereinafter the "Privacy Team") consisting of decisive team members of corporate and business unit processing personal data. The Privacy Team will regularly meet and will be supervised and organised by the DPO.

2. The Privacy Team will advise the DPO and prepare and approve any actions needed to become and/or remain compliant with data privacy legislation. Decisions made or actions taken may require formal approval by the Management Board.

V. DEFINITIONS

Data Protection Legislation has a language of its own. Some helpful definitions are set out below to

assist in understanding this Policy.

Consent - means an indication of data subject's wishes that is freely given, specific, informed and unambiguous by a statement or clear affirmative action that signifies agreement to the processing of his or her personal data.

Controller - means the person or legal entity (*e.g.*, company) who determines the purposes for which and the way in which personal data are processed. For instance, the particular TPV legal entity is likely to be the controller in respect of the personal data of its Staff.

Data Breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access of/to personal data that is transmitted, stored, or otherwise processed.

Data processor – means the natural or legal person, public authority, agency or other body (e.g. company) which processes personal data on behalf of the controller.

Data Protection Legislation - means the General Data Protection Regulation (EU 2016/679) and the ePrivacy Regulation (20-17) 10 (when it enters into force).

Data Subject - an identified or identifiable natural person or, in some EU Member States (*i.e.*, France, Belgium and Luxembourg), legal person (*e.g.*, companies).

Filing system - means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. This includes any manual records filed in an organised, logical way by reference to individuals or by reference to criteria reliant to individuals (*e.g.*, card-index system). Examples are ERP and CRM systems, such as SAP, Salesforce, Oracle; PIM solutions, such as Microsoft Outlook, Lotus Notes, including copies of information synchronised to mobile devices; simple lists stored in Microsoft Excel or Word, such as attendance/invitation lists for customer or press events.

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. Examples are "Name, address, telephone number, email address, birthday, anniversary, nickname, spouse/partner name".

Processing of personal data ("processing") - means any operation or set of operations which is

performed upon personal data, whether or not by automatic means (*e.g.*, computer, television set tablet or smart phone), such as collecting, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. For example, collecting the contact details of customers' contact persons and recording them in TPV's computer or card-index systems constitutes processing of personal data.

Profiling - means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Special or sensitive personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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.

Other definitions are set out in the body of the text where appropriate.

VI. PROCESSING OF PERSONAL DATA WITHIN TPV

1. TPV and all members of its Staff, as defined in the Introduction, may not Process Personal Data unless specifically permitted by this policy or pre-approved by the Managing Director, pursuant to a formal exception request.

2. Through the course of the following business activities, TPV and its employees may process personal data:
    1. Smart TV and Monitor production, supply, service and repair and sales activities. Specifically, employees may process or have processed personal data relating to provision of service, repairs, handling of security incidents, the registration and operation of Smart TV's (such as Smart TV IP-address, consumer-ID, device-ID's, store preferences, country and languages), customer behaviour, sensitive data, marketing and sales related data. They may also process personal data (anonymous or non-anonymous) in connection with analysis and online advertisements.
    2. Sales and Marketing. Employees may process personal data relating to commercial partners and customers (e.g., purchasers of TV sets, SSP's, ASP's), including through customer repair complaint tracking systems.
    3. Human Resources. Employees may process personal data relating to the hiring, compensation, benefits and related issues of TPV employees and applicants.

4. Other. Employees may process personal data relating to other relations, (e.g. suppliers, purchasers, complaints, etc.).

VII. COLLECTION AND PROCESSING OF PERSONAL DATA – TPV GENERAL PRINCIPLES

Data Protection Legislation lays down principles for the processing of personal data which must be complied with. In case of doubt as to the application of these principles in a particular case, the DPO shall be consulted.

(i). Lawfulness and accuracy of personal data

TPV will ensure that personal data shall be:

- processed fairly and lawfully; in particular, personal data shall only be processed on the basis of the relevant Data Protection Legislation;

- collected for specified, explicit and legitimate purposes and not processed further in ways incompatible with these purposes; TPV shall specify the purposes prior to commencing the processing of personal data;

- adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed; TPV shall ensure that the processing operations of personal data are designed so as to collect and further process only those data that are necessary. To the extent possible, use shall be made of the options of anonymizing or using pseudonyms (*i.e.*, replacing the name or another individual identifier by a substitute making the identification of the individual either impossible or considerably more difficult).

- accurate and, where necessary, kept up to date; TPV will take reasonable steps to rectify or delete personal data that are inaccurate, incomplete or outdated; in case Data Subjects are required to update their data themselves, TPV will remind them to review or update their personal data.

- kept for no longer than necessary for the purposes for which the data were collected and processed (*see*, Section VIII. below);

- processed in accordance with the Data Subjects' rights.

(ii) Processing personal data legitimately

1. Processing shall be lawful if one of the following applies:
    1. Data subject has unambiguously given his/her prior consent;
    2. Processing is necessary for the performance of a contract to which the data subject is party;
    3. Processing is necessary for compliance with a legal obligation;
    4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    6. Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

2. Consent Requirements for Processing Personal Data: Personal Data may only be processed in accordance with this policy if the Data Subject has given its voluntary, specific, informed and unambiguous consent to the Processing of its Personal Data. The Data Subject concerned shall be informed of the purposes of the processing for which consent is requested, the possible consequences of the processing for the Data Subject and other relevant details required to ensure fair processing prior to obtaining consent. Consent should be obtained through a statement or "clear affirmative action". Employees must use a consent form pre-approved by the DPO or Legal.

   Consent may be withdrawn at any time. In case the Data Subject has withdrawn his consent, TPV shall stop processing the personal data for the purposes for which consent was given and inform the Data Subject about the consequences of withdrawing his/her consent.

   In all other instances, prior approval from the DPO must be obtained before Processing Personal Data.

3. The Processing of special categories of personal data (Sensitive Personal Data) always requires the explicit consent of the Data Subject, prior to Processing the Personal Data. In any event, Sensitive Personal Data may not be processed, unless permitted by data protection legislation. Approval from the DPO is necessary before Processing of Special Personal Data without the explicit consent of the Data Subject.

4. Processing Personal Data of Customers for Marketing or Commercialising Purposes: where an employee intends to conduct direct marketing ytowards customers and collect Personal Data, the employee must obtain the customer's consent prior to receiving the customer's Personal Data ("opt-in"), unless this is obtained by an intermediate third party.

5 TPV will ensure that personal data are only processed if at least one of the criteria listed in Section 1 of this article is met. If you are not sure whether certain processing operations meet the above

criteria or prior to introducing a new data processing operation, please contact your DPO.

6 TPV has set up a processing register in which the systems and databases that TPV uses and in which personal data are processed are listed. The processing register is managed by the DPO and kept up-to-date by him/her or under his/her supervision.

(iii) Special categories of personal data

1. Certain personal data is given special status in Data Protection Legislation (sometimes called 'Special or Sensitive Personal Data'). Subject to the exceptions set out below, processing of such special categories of personal data is in principle prohibited. To a limited extent, TPV needs however to collect such data, in which case it will ensure that the Data Subjects concerned are informed of such collection and processing. Where required by law, the Data Subjects' explicit consent to the processing will be obtained. Without consent, the processing of such data is in principle only allowed if it is necessary for one of the following purposes:

- carrying out certain obligations or enforcing certain rights in the field of employment law in so far as the processing is authorised by national law providing for adequate safeguards;
- to protect the vital interests of the Data Subject or of another person;
- where the Data Subject is physically or legally incapable of giving his consent;
- the processing relates to data which are manifestly made public by the Data Subject; or
- the processing is necessary for the establishment, exercise or defence of legal claims.

Data Protection Legislation lays down more specific requirements and/or exemptions in addition to those mentioned above which supersede this Policy.

3. In case of doubt as to the legitimacy of the (intended) processing of data, please contact the DPO.

(iv) Transparency and provision of information to the Data Subjects

1. In principle, personal data shall be collected directly from the Data Subjects. When collecting personal data from the Data Subjects, the relevant TPV legal entity will provide the Data Subjects with at least the following information except where the Data Subject already has it:

- the identity and the contact details of the controller (in many cases, this will be the TPV legal entity which has initiated and owns the particular processing operations)
- the contact details of the data protection officer,
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, if any;
- Information concerning transfer personal data to a recipient in a third country (for example China)
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- where the processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the controller or by a third party;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Data Protection Legislation may lay down additional requirements and/or provide for certain exceptions to this obligation which supersede this Policy. The aforementioned information shall be easily understandable and may be provided by individual or general information.

2. If personal data are collected from third parties rather than the Data Subjects themselves or are passed to TPV for further processing, care must be taken to ensure that the Data Subjects are properly informed. For this purpose, fair obtaining clauses shall be included in all contracts with such third parties.

3. If an TPV entity introduces a new process or tool that will result in the processing of personal data beyond the purposes described in the relevant fair processing notice or in the information provided at the time of the collection of the personal data, the TPV entity will ensure that the Data Subjects concerned receive the information mentioned in Section 1 of this article with respect to the new process or purpose.

(v) Confidentiality and security of the processing according to art. 32 GDPR.

1. TPV undertakes to take the appropriate technical and organisational measures for the protection of personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. These measures shall apply to servers, computers, networks or other IT hardware as well as software applications and filing systems.

2. A general list of the technical and organisational security measures to be taken by each TPV legal entity can be found in Annex 1. Taking into account the state of the art and the costs of their implementation, these measures shall ensure an appropriate level of security appropriate to the personal data which are to be protected, depending on the nature of the categories of data and the risks associated with the intended uses. In order to ensure compliance with Section 1 of this article, TPV, its Staff and any third party which processes personal data on behalf of TPV shall also comply with the TPV IT policies, and other TPV policies relating to information security.

3. TPV will inform all Staff members about their obligations concerning this Policy by the appropriate means of communication, and will conduct training of the Staff regarding the protection of personal data.

4. Any person acting under the authority of an TPV entity who has access to personal data must not process them outside the scope of this Policy and only on instructions from the entity, unless she/he is required to do so by law. In addition, TPV will limit the access to the personal data to those necessary for the requirements of the processing. Only authorised personnel may process personal data after having signed a confidentiality undertaking. This requirement to sign a confidentiality undertaking shall apply at least to HR, database and IT administrators as well as to external contractors.

(vi) Data breaches and notification

Data Protection Act contains specific obligations for Controllers and Data processors regarding the notification to the Data Protection Authority of data breaches and in some case also to Data Subjects involved. In case of any data breach immediate internal action is required. A data breach is defined as any loss or illegal processing of personal data, in such a way that the technical and organisational security measures have not worked. In practice this could be anything from losing a USB-stick or laptop, to a hack of a system, computer virus, fire in a data centre or accidently sending an e-mail with personal data.

If a data breach has occurred it must be notified immediately, but in any case within 24 hours after the breach has been discovered, to the DPO, Legal department or manager. Thereafter it may have to be immediately notified to the Data Protection Authority and in case of certain circumstances also to the data subjects. In practice this has to be done at the 2nd day working day after after having

become aware of it of the breach. If this is not done, TPV may be subject to substantive fines.

(vii) Privacy by Design / Privacy by Default

TPV adheres to the objectives of Privacy by Design — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage, which may be accomplished by practicing 7 Foundational Principles, listed in Annex 2.

VIII. REGISTRATION

TPV will observe all mandatory registration obligations (including obligations to notify and/or request prior authorisation) towards the competent national authorities as required by the Data Protection Legislation. Every TPV entity must check whether and to what extent such registration obligations exist. In case of uncertainty, the DPO shall be consulted.

IX. DATA PROTECTION IMPACT ASSESSMENT

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, TPV shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. TPV has chosen to implement a Data Protection Impact Assessment (DPIA) structure, aiming at identifying and reducing privacy risks at an early stage. DPIA is the essential core of any sustainable data protection framework and a tool to measure privacy risks when developing ICT systems, applications and databases, and map these privacy risks in a structured and clear manner. The DPIA has the shape of a test model / questionnaire, containing both factual and technical questions as well as questions that aim to measure compliance with national and European legal requirements. The aim is to focus at an early stage on the intended processing of personal data that require attention and elaboration. In particular, the questionnaire is intended to both provide direction as well as to be corrective. It should also stimulate the answering process as such also awareness of different privacy concerns that must be considered when developing a system or database.

The DPIA is a responsibility of the business and must be completed at the early stage of any new projects. The completed PIA document can be obtained by the Data Protection Officer, completed and sent back, after which he/she will assess the document, approve or propose changes.

X. DISCLOSURE OF PERSONAL DATA

(i) Within the TPV group of companies

Under Data Protection Legislation, disclosure or otherwise making available of personal data to a third party is only allowed if one of the criteria for making data processing legitimate is met. Disclosure of personal data to another TPV entity is in principle considered as a transfer of personal data between two different entities, which is allowed only if the applicable legal requirements are met.

(ii) To data processors

1. TPV may need to disclose or transfer personal data to selected external third parties that they have hired to perform certain processing operations on their behalf, for instance, pension scheme or insurance providers, bankers, medical, ICT, cloud service providers and other professional advisers, travel agents, rental agencies and other third parties and which act as data processors.

2. Data processors may only be granted access to personal data if appropriate contractual arrangements have been made that require the data processors to process the personal data solely for the purposes of performing the services specified in the applicable service provider agreement and only in accordance with the instructions of the TPV entity in question or to make decisions regarding the personal data as part of the delivery of their services. The data processors must also undertake to put in place appropriate security measures to keep the information which is disclosed safe and confidential and ensure compliance with those measures. TPV will take appropriate actions, if it finds that a data processor does not comply with his obligations. A generic example of a data processing agreement shall be provided by the DPO.

3. TPV will select reliable suppliers and will perform due diligence in contracting them for the processing of personal data.

(iii) To data controllers

TPV may be obliged to disclose certain personal data to other third parties, for instance, due to statutory obligations (*e.g.*, under tax or social security law). In these cases, TPV will, where appropriate, only disclose the personal data according to data protection guarantees in a contract, stipulating the measures to be taken by and obligations of such third party, or which may include restrictions as to the use of such personal data in order to protect the legitimate interests of the Data Subjects.

(iv) Outside the European Economic Area("EEA")

In certain cases, personal data may need to be transferred to countries outside the EEA (which

consists of 28 EU Member States (+ Iceland, Liechtenstein and Norway). Most of these non-EEA countries are not considered to provide an adequate level of protection for personal data and, aside from an increasing number exceptions, personal data may only be transferred to such countries if a contract has been concluded between the transferor and the recipient that adduces adequate safeguards. Prior to transferring any personal data to someone outside the EEA or in case of questions, please consult your DPO.

XI. RETAINING PERSONAL DATA

1. TPV shall specify in a retention policy the maximum period for which personal data will be retained in accordance with the legislative requirements in force at the time.

2. TPV must not hold personal data longer than is necessary and, accordingly, shall ensure that after the maximum retention period has expired, the personal data are either deleted; anonymized so they can still be used for statistical and similar purposes; or archived where they may be used for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes.

XII. RIGHTS OF DATA SUBJECTS

1. Under Data Protection Legislation Data Subjects have different rights, subject to certain exemptions and restrictions. TPV will respect the rights of Data Subjects in accordance with the applicable Data Protection Legislation. These rights include the following rights:

(i) Right of access

Any Data Subject has the right to request access to his/her personal data held by TPV. Where required by law, TPV will inform the Data Subject at reasonable intervals and without excessive delay or expense, as to:

a) the purposes of the processing;
(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(ii) Right to have personal data rectified

If personal data are inaccurate or incomplete, the Data Subject may request that his/her personal data be rectified. It is every Data Subject's responsibility to provide TPV with accurate data about him or her and to inform TPV of any changes.

(iii) Right to have personal data erased and/or blocked.

If the processing of the personal data does not comply with the Data Protection Legislation, the Data Subject may request that the data be erased and/or blocked.

(iv) Right to object

Data Subjects may object, in accordance with the Data Protection Legislation, to the processing of personal data relating to them on compelling legitimate grounds relating to their particular situation, save where otherwise provided by national legislation. TPV shall respect the right to object in case of direct marketing.

(iv) Right to be forgotten

Data Subjects in some case have the right to claim full erasure of their data in case they have legitimate grounds. Please consult the DPO in such a case.

(vi) Automated individual decisions

Data Subjects have the right not to be subject to a decision which produces legal effects concerning them or significantly affecting them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to them such as their performance at work, creditworthiness, reliability, conduct, *etc*. If such automated decisions are made, the Data Subject shall be granted the opportunity to express his/her point of view, unless the processing is authorised by a law which also lays down measures to safeguard the Data Subjects' legitimate interests.

(vii) Profiling ad art. 4 GDPR

In the processing of personal data, profiling may be used. Profiling concerns any form of automated processing of personal data whereby on the basis of personal data certain personal aspects of a natural person are evaluated, in particular with the intention of his professional achievements, economic situation, health, personal preferences, interests, reliability, behavior, location or to analyze or predict movements. The data subject shall have the right not to be subject to a decision based exclusively on automated processing, including profiling, which has legal effects on him or which otherwise affects him to a significant degree. Furthermore, the person concerned always has the right to object to profiling due to his specific situation. TPV's policy is aimed at transparency of algorithms and the prevention of automated decisions

(viii) Copy of the personal data undergoing processing

TPV shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, TPV may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(ix) Right to data portability ad art. 20 GDPR

The right to data portability means that data subjects can receive the personal data that they have provided to a controller in a structured, current and machine-readable format and can transfer these to another controller. This new right aims to strengthen the position of the data subject concerned and give him / her more control over his / her data. This right is limited to the personal data provided by the person concerned and therefore not for derived personal data. If such a request reaches TPV, TPV has the obligation to process the request within 30 days, it is therefore of great importance that the request is sent immediately to the DPO.

2. A Data Subject who wishes to exercise his rights should make a written request (which shall include e-mail) to the DPO of his TPV entity.

3. TPV will inform third parties to whom personal data have been disclosed of any rectification, erasure or blocking carried out in compliance with the Data Protection Legislation, unless this proves impossible or involves a disproportionate effort.

XIII. EMPLOYEES RESPONSIBILITIES

1. TPV's Staff are expected to adhere to this Policy and to ensure that those for whom they are responsible also adhere to this Policy.

2. Staff must become familiar with the aims of this Policy and follow the provisions set out therein. In

particular Staff should:

- seek advice from their superior, the relevant DPO or Legal department where they have any doubts as to whether or not the processing of personal data that they are required to carry out in the course of their employment complies with the Data Protection Legislation or with this Policy;

- process personal data that they process in the course of their employment only as a part of his/her duties to TPV and only for those specific purposes that have been expressly determined by TPV;

- provide all assistance to the DPO;

- not keep duplicate records of any personal data where a centralised filing option is available. By keeping own records unnecessarily, this can complicate the process of responding to subject requests;

- notify their superior immediately should they detect any potential or actual breach of the Data Protection Legislation.

XIV. ENFORCEMENT

All TPV entities will ensure that this Policy is observed. All persons who have access to personal data processed by TPV must comply with this Policy. Non-compliance with this Policy may lead to appropriate disciplinary sanctions, including dismissal or any other kind of sanction permitted by applicable law, notwithstanding any further civil or criminal action that may be taken.

XV. MONITORING AND REVIEW

TPV reserves the right to modify this Policy in response to its statutory obligations or requirements imposed by data protection authorities. If TPV makes changes to the Policy, TPV will inform the Data Subjects concerned of any material changes in the Policy.

XVI. QUESTIONS OR INQUIRIES

1. Any questions or inquiries regarding this Policy or, more generally, the protection of personal data should be addressed to the competent DPO or Legal.

2. Any TPV company shall inform the DPO immediately of any legal requirements applicable to it

prohibiting it from complying with this Policy.

XVII. ENTRY INTO FORCE

This Policy will enter into force as of 1 January 2017 and will be subject to review before 31 December 2018.

ANNEX 1

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Each TPV legal entity shall take technical and organisational security measures with respect to:

(1) physical access control;
(2) control of use and access to data;
(3) control of data transmission;
(4) input control; and
(5) availability control.

These measures shall apply to all data processing systems (whether automated or filing systems), servers, computers, networks or other IT hardware as well as software applications.

In addition, all Staff must comply with the IT security policy (and any other policies relating to security) set forth by or on behalf of TPV. These policies shall be considered an integral part of the Data Protection Policy and this Annex. Compliance with this Annex and these policies will be regularly monitored and checked. Staff will be trained (on an on-going basis) in security and risk management in relation to personal data.

(1) Physical access control

TPV shall take measures to prevent unauthorised persons from gaining access to data processing systems with which personal data is processed. For this purpose, TPV shall (i) take measures to secure the premises; and (ii) take security measures within the building. TPV shall take one or more of the following measures:

(i) <u>Measures to secure the premises:</u>

- ensuring physical security of the premises (*e.g.*, fences, gates or other);
- securing entries and exits (including emergency exits, balconies, *etc*.) and locking doors;
- protecting windows (on both the ground and first floors);
- supervising the premises/building outside of office hours (*e.g.*, security guards, alarm system, secure locks, CCTV);

- using an entry control system to the premises/building (*e.g.,* passport / other ID / swipe card / swipe card with key administration and documentation), which make provision in case of loss;
- registering and restricting access to visitors (*e.g.*, visitor's passport, accompanied visits);
- developing and implementing organisational rules on access by (and monitoring of) external service providers and their personnel (*e.g.*, prior identification, authorisation, confidentiality undertakings, accompanied visits).

(ii) Security measures within the building:

- implementing security measures at the reception;
- developing different levels of access in the building (*e.g.*, supervised areas with restricted access on a "*need to know*" basis);
- alarm system;
- increasing workstation security (*e.g.*, restricted access to the server room, machine room, telecommunication system);
- locking offices at night or during absence;
- locking filing systems, notebooks or other mobile data carriers in cupboards or containers at night or during absence;
- physically protecting hardware (*e.g.*, locking of drives) and mobile IT equipment;
- using physical barriers around data processing devices (*e.g.*, computer screens) to prevent viewing by unauthorised persons.

(2) Control of use and access to personal data

TPV shall take measures to protect data processing systems from unauthorised use. TPV shall also ensure that persons entitled to use a data processing system only have access to the personal data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorisation (either in the course of processing / use or after storage). To safeguard against unauthorised use of data processing systems, TPV shall take one or more of the following measures:

- maintain all electronic personal data on systems that are protected by secure network architectures that contain protective devices, such as passwords, firewalls and intrusion detection devices;

- ensure that only individuals who are subject to confidentiality obligations are given access to personal data through the use of a unique identifier and password;
- maintain an up-to-date user account management to ensure that individuals are only given access to information that is necessary for the performance of their job duties and in connection with their specific roles or responsibilities; and include details of who is given access to such systems (including a clear definition of owners, user rights and access rights; different levels of authorisation, file/directory missions/access; technical realisation, logging/monitoring of user access, access review and controls; clear procedures for the delegation of access rights in case of absence; separation of functions; special precautions with consultants and temporary employees who should only be granted limited access to personal data, if any; *etc*.);
- leaver policy/checklist;
- system administration (including administration concept, different levels of administrator rights, identification and authentication, four-eyes principle, log of administration security, *etc.*);
- deactivation of connections that are not in use;
- user identification and authentication;
- password convention (including minimum length with use of both numeric and letters characteristics; no trivial words; special signs or figures; validity/days, *etc*.), documentation, control of use and regular checking of compliance (including blocking when repeated fail attempts, protection of authorisation/password tables against unauthorised access (such as encryption of sensitive personal data), *etc*.);
- prohibition of use of private hardware and software, unless this is specifically authorized;
- release procedure for software and programming guidelines;
- automatic log off periods;
- screensaver protection;
- clean desk policy;
- security violation monitoring and regular assessment of logs (login attempts, successful, failed);
- physical protection of hardware as well as (mobile) IT equipment, tablets, Smart phones;
- password protection for server booting;
- copy protection for user terminals (*e.g.*, no Disc terminal, no USB, no DVD burner, disc-lock, download or copy function deactivated);
- minimise network or boot services;
- kernel tuning;
- regular and PEN / vulnerability tests;

- standard intrusion detection software on all hosts;
- internet connectivity (including approved access points, firewall, authorisation of connection to the intranet, log internet traffic (outbound, inbound, by source and destination); ability to stop internet access services (hacker); documented escalation and communication process; internet web browsing protections; security incident response team);
- change program management;
- effective safeguards for system access and data transmission in case of telecommuting, in particular securing home computers/office (including company provided hardware and software, approved point of access, hardened operation system, regular vulnerability testing, monitored access, turn off file sharing and web browsers, strong passwords, real-time virus protection enabled, firewall, *etc*.);
- desktop/laptop/smart phone/tablets policy;
- regular reviews of e-mail and internet logs;
- locating computer monitors, printers, fax machines and copiers in such a manner that no unauthorised person can access personal data;
- secure deletion of personal data and secure disposal of IT equipment, hardware, data carriers and paper records (*e.g.*, removal of personal data from media and mobile data carriers prior to disposal and shredding of paper documents).

(3) Control of data transmission

TPV shall take measures to ensure that personal data cannot be read, copied, modified or removed without authorisation during electronic transmission or transport or cloud storage / processing, and that it is possible to check and establish to whom the personal data will be transmitted. For this purpose, TPV shall take one or more of the following measures:

- clear rules for the automated transfer of personal data (including kind/quantity, purposes, position/posts) and manner of transfer (*e.g.*, modem/telephone network, internet, fixed line, other);
- identification and authentication of recipients (for instance, by automatic call back, call number identification, ID, password, delivery note or other);
- logs of data transfer and regular assessment;
- encryption of electronic data;
- defence against unauthorised access from the telecommunications network (*e.g.*, firewall or other);

- logs of mobile data carriers (*e.g.*, hard disc, tapes, laptops, smart phones, tablets DAT, CD-ROM, DVD, USB sticks) which are securely stored and regularly controlled for their completeness and authenticity, including control on removal, copying, destruction and security during transport (*e.g.*, encryption or locked container, renowned transport companies);
- remote maintenance (*e.g.*, user administration, remote maintenance concept, identification and authentication, routing, connection, encryption of data at transmission, control of privileges, logs of remote maintenance and regular review);
- protection of servers against the unauthorised transfer of data between different security domains (*e.g.*, password protection for the server booting, monitoring of external maintenance personnel, control of remote maintenance);
- general prohibition on removing personal data from the office premises;
- copy-protect user terminals (*e.g.*, no floppy disk terminal; no CD burner; hard disk-lock; download/copy function deactivated);
- policy on destruction and deletion of personal data (including with respect to hard discs, media, mobile data carriers and paper).

(4) Input control

TPV shall take measures to ensure that it is possible to check and establish whether and by whom personal data has been input into data processing systems, modified or removed. For this purpose, TPV shall take one or more of the following measures:

- input logs/audit trails (for files and/or data fields) without the possibility to switch off this function, and regular log assessments;
- keeping e-mail and internet logs;
- making the modification of databases generally subject to specific authorisations.

(5) Availability control

TPV shall take measures to ensure that personal data is protected from accidental destruction or loss. For this purpose, TPV shall take one or more of the following measures:

- operational availability;
- secure architecture for web- and backend servers;
- operating system security;
- risk analysis and prevention measures;
- implementation, regular testing and maintenance of emergency concept, business continuity and disaster recover plan, contingency planning and true failsafe procedures as well as Staff training;
- Uninterrupted Power Supply (UPS), secured power supply (generators), overvoltage protection;
- fire alarm and protective measures;
- intrusion detectors;
- emergency switches;
- virus protection;
- security patches and hotfixes;
- storage of servers in locked burglar/fire/waterproof rooms which are generally capable of withstanding adverse conditions (safeguards against booting of the servers are in place);
- regular backup of personal data stored, including on servers, C-drives and inboxes;
- backup recover and retention (including backup media management and controls, routine backups, secure and controlled off-site storage of backups, procedures to govern maintenance, rotation and retention, *etc*.);
- data records retention policy;
- prohibition on storing personal data on computer hard discs if these are not automatically backed up;
- download policy.

ANNEX 2

PRIVACY BY DESIGN

1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy Embedded into Design

Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.