General Data Protection Procedure

Transported Asset Protection Association Europe Middle East and Africa (TAPA EMEA)

Procedure Number:	1
Revision Number:	0
Date of issue:	April 2018
Status:	Approved
Date of approval:	April 2018
Responsibility for procedure:	Data Controller
Responsibility for implementation:	Data Controller
Responsibility for review:	Data Controller
Data Controller	Laurence Brown
Date of last review:	April 2018
Date of last revision:	0
Date of next review:	April 2019

Contents

Background

1 Our **Mission** describes why the Transported Asset Protection Association (TAPA), a not for profit organization, exists; It declares our purpose. Our **Vision** outlines our hopes for the future, a picture of our desired state. Our **Values** are the beliefs we share in the organization. They drive TAPA's culture and provide a framework in which decisions are made.

Mission:

TAPA's mission is to minimise cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats.

Vision:

TAPA's vision is an international supply chain where controlled and traceable products can be transported in a cost efficient and secure environment.

Values:

- Integrity and Transparency in everything we do.
- Information sharing between those with different opinions, backgrounds or experiences.
- Owning our Standards, Actions and Decisions.
- Representation and support for all of our stakeholders.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union.

The General Data Protection Regulation (GDPR) proposed by the European Commission will strengthen and unify data protection for individuals within the European Union (EU), whilst addressing the export of personal data outside the EU.

A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

The regulation provides a separate definition for "sensitive personal data". This relates to information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual orientation, or details of criminal offences.

Today, the EU definition of "personal data" is set out in the Data Protection Directive 95/46/EC. It defines personal data as "any information relating to an identified or identifiable natural person" (Art.12 Oct 2015)

TAPA EMEA is committed to:

1) protecting personal data of members, clients and personnel from unintended loss, destruction, damage, modification, disclosure or other security risk, and
2) to processing personal data of clients and staff fairly and lawfully in accordance with current data protection legislation

2 Definitions

Data Protection legislation has a language of its own. Some helpful definitions are set out below to assist in your understanding of this Procedure:

Association's Personnel – includes all Elected Directors, Employees, Contractors and Associates

Association's Members – members as defined by the Association's constitution

Data Controller – means a person or company who decides the purpose for which and the way in which personal data is processed.

Data Records – all records stored electronically on any database operated or used by the company or any of the tools it may use – see list

Data Protection Officer – See Data Controller

Data Subject – any individual identified as the Association's personnel and Member or is a client.

Personal Data – means information about a living person who can be identified by that information or by that information together with other information that the Data Controller has or is likely to obtain.

TAPA EMEA - Transported Asset Protection Association covering the region of Europe, the Middle East and Africa.
Other definitions are set out in the body of the text where appropriate.

3 The Procedure:

This Procedure aims to:

3.1 Set out practical guidelines on the General Data Protection Regulation.

3.2 Indicate responsibilities in relation to the processing of personal data.

3.3 Prevent unfair or unlawful processing of personal data by, for example, unauthorized retention, disclosure, modification or destruction.

3.4 This Procedure is a TAPA EMEA procedure and indicates how all personnel engaging in activities on behalf of the Association will address data protection issues for both TAPA EMEA and its members.

3.5 All data will be processed in compliance with the Data Protection Principles - namely

Personal data must:-

3.5.1 Be processed fairly and lawfully.

3.5.2 Be obtained only for one or more specified or lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.

3.5.3 Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

3.5.4 Be accurate and, where necessary, kept up-to-date.

3.5.5 Be processed in accordance with the rights of data subjects, namely only used in accordance with permissions granted.

3.5.6 Be restricted to authorized persons only.

3.5.7 Be protected by appropriate technical and organizational measures against unauthorized or unlawful processing, against accidental loss or damage.

3.5.8 Personal data will not be transmitted over the internet unless appropriate encryption methods are used or by consent of the data subject.

3.5.9 Personal data will not be sent to a third party on portable storage media or in paper form by conventional post. A secure delivery service must be used, unless consent is given by the data subject.

3.5.10 Personal data should not be stored on laptops unless this is unavoidable and appropriate security measures have been implemented following a risk assessment. This will comprise an encryption and security system. These measures will apply to portable data storage media such as DVDs, mini hard disk drives and USB flash memory data sticks.

3.5.11 TAPA EMEA will not keep data for longer than is necessary and will take all measures available to it to destroy any data held by deleting the records and shredding any paper records held, unless retention of the information, documentation is required under local law.

3.5.12 TAPA EMEA will destroy all notes made during telephone conversations, which contain personal data as soon as possible after the conclusion of the call unless the information is required in pursuance of any legal requirement

3.5.13 TAPA EMEA will take all reasonable steps to ensure the safe storage of any data by using a number of technical methods (i.e. firewalls, encryption, password protection,) for electronically held data or organizational methods (hierarchy of access to personnel files, locking cabinets etc.) for any paper records, protecting personal data where the importance of the personal data makes this appropriate

3.5.14 All TAPA EMEA personnel who have access to personal data controlled by TAPA EMEA whether or not on computer, and whether in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that TAPA EMEA, nor any individual employed by TAPA EMEA, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data.

4 Personnel Responsibilities

All Association's personnel must fully comply with all TAPA EMEA procedures and requirements in regards to personal data, in that:

All Association's personnel who have access to personal data controlled by TAPA EMEA, whether or not on computer, and whether in the office or at home or elsewhere, must take adequate precautions to ensure confidentiality so that TAPA EMEA, nor any individual engaged by TAPA EMEA, becomes exposed to criminal or civil liability as a result of the loss, destruction or disclosure of personal data. All individuals must fully comply with all TAPA EMEA procedures and requirements in this regard.

In addition

4.1 Laptops are particularly vulnerable to theft, especially when used outside of TAPA EMEA premises. In these circumstances, Association personnel must keep laptops in their possession at all times unless they have been deposited in a secure location such as a locked closet or a hotel safe.

4.2 Association personnel must notify changes of name, address, telephone number, bank and marital status to the Executive Director of TAPA EMEA as soon as possible. The Executive Director of TAPA EMEA will endeavor, periodically, to ask staff to confirm that such personal data held by TAPA EMEA is accurate.

4.3 If any Association personnel receive any letter from a member, business contact, other colleague, or any other third party requesting any information about them then they must pass the letter to the Data Protection Officer, i.e the Data Controller immediately. In TAPA EMEA this is Laurence Brown.

4.4 Association personnel should ensure security of personal data (whether paper records or electronic) at all times, including outside of any premises operated by TAPA EMEA or by a third party on behalf of the Association

4.5 Association personnel must not leave personal data on screen or on desk tops when they are not at their desks. Paper records should be stored securely unless under active consideration. A clear desk policy should be observed when staff leave the office for the day. Computers, Laptops should be hibernated whilst equipment are left unattended

4.6 TAPA EMEA expect all Association personnel to use computers, email and the internet responsibly and in accordance with the data protection principles. Association personnel should make themselves aware of the provisions contained in the TAPA EMEA internet and e-mail Acceptable Use Procedure and Policy. (See Annex A)

4.7 Association personnel are expected to adhere to this procedure as laid out in section 3 and to ensure that those for whom they are responsible both adhere to this policy and protect computer systems and personal data from security risks. Where necessary, Association personnel should seek advice from the IT support to assist in these goals.

4.8 Association personnel will be authorized to gain access to certain computer systems, programs and data. No Association personnel must attempt, alone or with others, to gain access to data or programs to which they have not been authorized to gain access.

4.9 Association personnel must become familiar with the aims of the procedure as laid out in section 3 and follow any guidelines set out.

In particular staff should:

- Seek advice from an Executive Director or the Data Controller where they have any doubts as to whether or not the processing of personal data that they require to carry out in the course of their engagement complies with the Act;

- Not use personal information that they hold in the course of their role or any reason other than the performance of their duties. To procure personal information from TAPA EMEA and use it without its consent is likely to constitute a criminal offence under the Act;

- Provide all assistance to the Data Controller in the conduct of any audit or preparing a response to a subject access request;

- Keep information that they process for TAPA EMEA safe and secure in accordance with any procedures issued by TAPA EMEA. Where no procedures are set out explicitly, you should exercise a degree of care over the personal data that you process by considering the harm that may result were the information to be disclosed unintentionally. Guidance on appropriate levels of security can be obtained from the Data Controller.

- Not keep duplicate records. Keeping your own records unnecessarily can complicate the process of responding to subject access requests.

- Notify the Data Controller immediately should you detect any potential or actual breach of the Act.

4.10 Any breaches of this Procedure in relation to personal data security will result in disciplinary action and, in serious cases, may result in the dismissal of Association personnel.

5 **Association Personnel and Members' Data**

Personal data about an individual who wishes to be part of the Association Personnel and members will be processed for various purposes which may include:

5.1 To assess his/her application to become a member of the Association's personnel;

5,2 To administer the contractual sick pay system;

5.3 To address any health and safety issues;

5,4 To facilitate management decisions;

5,5 To detect fraud;

5.6 To administer any personal health insurance benefit or other similar benefit;

5,7 To market TAPA EMEA services;

5,8 To form part of any TAPA EMEA tenders / contracts or promotions;

5.9 To assist in the administration of finances;

5.10 To administer funds and finances of a third-party client;

5.11 To administer the employment relationship so that TAPA EMEA may properly carry out its duties, rights and obligations to the employee;

5.12 To assess an application to become a member of the Association. Any checks and data held will be limited to that which is attributable to their status within the organization applying for membership

6 Sensitive Personal Data in relation to Association Personnel only

6.1 Certain personal data is given special status in data protection legislation. This personal data is called sensitive personal data. Sensitive personal data is personal data consisting of information as to:-

6.1.1 racial or ethnic origin.

6,1.2 political opinions.

6.1.3 religious beliefs (or other beliefs of a similar nature).

6.1.4 trade union membership.

6.1.5 physical or mental health.

6.1.6 sexual orientation.

6.1.7 commission or the alleged commission of an offence.

6.1.8 proceedings for any offence, the disposal of such proceedings or the sentence of any Court in such proceedings.

6.2 Subject to the exceptions set out below and elsewhere in this procedure, sensitive personal data shall generally only be processed after company personnel / clients has given express consent. TAPA EMEA may in certain situations process the data without consent if it is necessary for processing to take place for one of the following purposes:-

6.2.1 ensuring health and safety of staff;

6.2.2 ensuring a safe working environment;

6.2.3 maintaining records of statutory sick pay or maternity pay;

6.2.4 protecting the person and property of people entering on to the premises of TAPA EMEA;

6.2.5 carrying out any other obligation or enforcing any right under employment law;

6.2.6 Participating in legal proceedings or obtaining legal advice;

6.2.7 For the administration of justice;

6.2.8 For medical purposes by a health professional;

6.3 Sensitive personal data relating to racial or ethnic origin may be processed without express consent in order to monitor the effectiveness of TAPA EMEA's Race Equality Policy and Procedure.

7 Requests for Information

An individual about whom TAPA EMEA holds personal data has the right to be told whether their personal data is being processed by or on behalf of TAPA EMEA or a third party client and, if so, to be given a description of:

i. the personal data held;
ii. the purposes for which it is being processed and;
iii. the recipients of the personal data;

Given a copy of the personal data in an intelligible format (unless to do so is disproportionate or the person has agreed to an alternative way of providing access) and is not subject to any legal proceedings

Given any information available regarding the source of the personal data which would not breach any client confidentiality provisions

TAPA EMEA is entitled to require the individual to pay a fee of up to €10for any subject access request.

All requests should be in writing. Requests should be directed to the Data Controller namely Laurence Brown. Any company personnel receiving such a request should pass these on with immediate effect

The request for information will be dealt with promptly and in any event within 40 days from TAPA EMEA receiving it and contain:

1) the written request for the personal data;
2) sufficient details to allow TAPA EMEA to respond to it;
3) sufficient details to confirm the identity of the person making the request; and
4) a payment of €10.00 where requested.

Where the provision of information would reveal the identity of a third party, the information may not be provided unless either the consent of that third party is obtained or it is reasonable to proceed without their consent.

8 Restrictions on supplying personal data

Personal information relating to company personnel and clients cannot normally be disclosed to an unauthorized third party. These include family members, friends, local authorities, government bodies and the police. There are only certain circumstances when personal information can be given to such third parties and these include:

1) prevention or detection of a crime
2) apprehension or prosecution of offenders
3) prevention of serious harm to a third party
4) protection of the vital interests of the data subject, e.g. release of medical data where failure could result in serious harm or death
5) ensuring health and safety

Company Personnel have the right to expect documentary evidence to support such requests.

9 Management of Personal Data

Where TAPA EMEA takes any decision which significantly affects any Association personnel or Association members exclusively upon the results of an analysis of his/her personal data carried out by automated means then TAPA EMEA will provide that person with notice of this fact as soon as reasonably practicable thereafter.

If the decision is connected with a contract entered into between TAPA EMEA and another person or is taken for the purposes of considering whether to enter into or with a view to entering into such a contract, the other person will be allowed to make representations on the outcome of that decision

In the event of a potential intended or actual transfer of business information, TAPA EMEA will take all reasonable steps to limit disclosure of personal data about employees to any of the third parties concerned by for instance, the omission of names or other identifying particulars.

10 Data Controller responsibilities

The Data Controller must ensure that the Association personnel are aware of the aims of this procedure and follow the guidelines set out.

Provide all assistance to the Elected Directors of the Association and conduct any audit for preparing a response to a subject access request;

Not procure personal information from TAPA EMEA and/or use it without consent. To do so is likely to constitute a criminal offence under the Act.

11 Miscellaneous

TAPA EMEA has a legitimate interest in monitoring the behaviour of its Association personnel.
For instance, TAPA EMEA may wish to carry out monitoring in order to:

1) Detect harassment or other inappropriate behaviour;
2) Monitor performance of its staff where this is appropriate;
3) Monitor and detect the outward transmission of confidential information;
4) Prevent and detect theft of TAPA EMEA property;
5) Prevent or detect any unlawful act;
6) Monitor adherence to this and other policies;
7) Perform other duties in employment law;

Monitoring can take several forms. It can involve monitoring by way of Closed Circuit Television (CCTV), e-mail and Internet monitoring or telephone monitoring.

TAPA EMEA may hold information on the destination and duration of calls made from TAPA EMEAs telephone system and may use this information if misuse of the system is suspected.

12 Personal data - removal of personnel and members

Personal data will be removed immediately when personnel or a member leaves the Association and deleted from all software platforms listed in section 14, unless required by local law

13 Privacy Notice

See annex B for privacy statement which is posted on its website www.tapaemea.org

14 List of software platforms which hold personal data of personnel and members

TAPA EMEA website CMS
TalentLSM training tool
TAPA Conference App
TAPA IIS database
TAPA secure parking online tool
Certification Online Tool
TAPA message to members communication tool

Annex A - TAPA EMEA Internet and E-mail Acceptable Use Procedure and Policy.

Whilst engaged in the activities to the service provided to the Association, TAPA EMEA personnel must not breach any laws known to them in using any of the material they access

In particular, **Association personnel agree** not to do the following:

- Deliberately visit, view or download any material from any website containing pornographic, abusive, racist, violent or illegal material or material which is offensive in any way whatsoever.

- Download any images, text, sound or other material that is in breach of copyright.

- Upload or make available to others any material that is offensive, obscene, indecent, or which infringes the copyright of another person (e.g. images, MP3 and other audio and video files

- Upload or forward any subject data or other Association material to a personal email address or private storage facility without written permission from the Data Controller

- Use the internet for any illegal activity or gambling.

- Use the internet to harass, cause annoyance, inconvenience or anxiety to others. Examples would include abusive or offensive emails, spamming, distributing information regarding the creation of and sending internet viruses, worms, Trojan Horses, pinging, flooding, or denial of service attacks.

- Access, or attempt to gain access to, computer systems, data or resources to which they are not authorized, such as connecting to other users' resources.

- By using the service provided by the Association you agree to respect the Privacy of others.

- Access network services in such a way as to deny reasonable access to the network for other users, for example, by excessive use of network bandwidth. This could include the use of FTP servers, file-sharing software and video streaming.

- Attempt to gain unauthorized access to restricted part of the network or attempt to undermine the integrity or security of any computer systems or network.

- Association personnel are responsible for any damage caused to the computer equipment arising out of any willful act or negligent misuse.

Annex B - Privacy Policy (to be listed on the website)

General statements

Statement on the data controller:

Company:	Vereniging TAPA EMEA
Executive Director:	Laurence Brown
Address:	Rhijngeesterstraatweg 40D, 2341BV Oegstgeest, The Netherlands

Contact Data Protection Officer: laurence.brown@tapaemea.org

General information about data processing

Affected data:

Personal data is only collected if you inform us of this yourself. In addition, no personal data is collected. Any processing of your personal data that goes beyond the scope of the statutory permission is only possible on the basis of your express consent.

Processing purpose:	Association's work
Categories of recipients:	Public authorities subject to priority legislation. External service providers or other contractors. Other external bodies as far as the data subject has given his consent or a transmission of predominant interest is permitted.
Third-country transfers:	Contractors from outside the European Union may be used to fulfil and implement contracts.
Length of data storage:	The duration of the data storage is for the life time of membership or the Association personnel are engaged with the Association unless impacted by local law

Specific information about the website

Server logs

We collect data about access to the site and save it as ‚server log files'. The following data is logged:

- Visited site
- Time of day at the time of access
- Amount of data sent in bytes
- Source / link from which you came to the site
- Browser used
- Operating system used
- IP address used

Data collected are for statistical purposes only and are used to improve the website. However, the operator of the website reserves the right to retrospectively check the server log files in case of concrete evidence that points to unlawful use.

Use of a newsletter

As part of the registration to our newsletter, you provide us with your e-mail address and optional additional data. We use this information exclusively to send you the newsletter. Your data provided during the newsletter registration process remains with us until you unsubscribe from our newsletter. It is possible to unsubscribe at any time by using the link provided in the newsletter or by sending us a separate email. By unsubscribing, you deny us the right to use your e-mail address.

In addition, we use your e-mail address, which we receive in connection with the other communications we send out informing the members of our activities unless you have expressly objected to this type of usage. You may object to the use of your e-mail address at any time. Your objection (and thus the cancellation of our newsletter) can be submitted to us by sending an appropriate message to our e-mail address info@tapamea.org

Use of Google Analytics

This website uses Google Analytics, a web analytics service provided by Google Inc. ("Google"). Google Analytics uses so-called "cookies", i.e. text files that are stored on your computer and that allow for an analysis of your use of the website. The information generated by the cookie about your use of this website is usually transmitted to a Google server in the United States and stored there. However, if IP anonymisation is activated on this website, your IP address will be shortened by Google beforehand within member states of the European Union or other parties to the Agreement on the European Economic Area. The complete IP address will only be sent to a Google server in the United States in exceptional circumstances and then shortened there. On behalf of the operator of this website, Google will use this information to evaluate your use of the website, to compile reports on website activity and to provide other services related to website activity and internet usage to the website operator. The IP address provided by your browser as part of Google Analytics will not be merged with other Google data. You can prevent the storage of cookies by using the respective settings in your browser; however, please note that you may not be able to use all the features of this website if you decide to do so. In addition, you may prevent the collection of the data generated by the cookie that is related to your use of the website (including your IP address) as well as the processing of this data by Google by downloading and installing the browser plug-in available under the following link [http://tools.google.com/dlpage/gaoptout?hl=de]. Related to the discussion about the use of analysis tools with complete IP addresses, we would like to point out that this website uses Google Analytics with the extension "_anonymizeIp ()", therefore IP addresses are only processed in a shortened form to rule out a direct personal reference. For browsers on mobile devices, you can click this link [Link] to prevent the anonymous collection by Google Analytics on this website by means of a so-called "opt-out cookie".

Use of own cookies

This website uses its own cookies to enhance user-friendliness ("cookies" are data records sent by the web server to the user's browser for later retrieval). Our cookies do not store any personal data. You can generally prevent the use of cookies by prohibiting the storage of cookies in your browser.

Please find more information about our cookies here: [LINK]

Google Web Fonts

This website uses Google Web Fonts. When you access the page, fonts are retrieved from an external Google server in the United States to make the page more visually appealing when it is shown in your browser. Unfortunately, it is currently unknown whether Google logs this server request and continues to use the collected data. However, it can be assumed that the Google privacy policies (http://www.google.de/intl/de/policies/privacy/) apply. This means that your IP address will be stored for several months.

Fonts.net

On our site, JavaScript code is downloaded from Monotype Inc., Monotype, 600 Unicorn Park Drive, Woburn, MA 01801, USA (Fonts.net). This code is used to represent fonts. If you have activated JavaScript in your browser and have not installed a Java Script Blocker, your browser may transfer personal data to Fonts.net. We do not know what data Fonts.net associates with the data received and for what purposes Fonts.net uses that data. More information can be found in the Fonts.net privacy policy: http://www.monotype.com/legal/privacy-policy.

Details of other data processing methods

Specific information on applications for admission

Affected data:	Details of the company in the admission process
Processing purpose:	Implementation of the admission process, administration of memberships
Categories of recipients:	Public authorities subject to priority legislation. External service providers or other contractors. Other external bodies as far as the data subject has given their consent or a transmission of predominant interest is permitted.
Third-country transfers:	Contractors from outside the European Union may be used to fulfil and implement contracts.
Duration of data storage:	Application data will generally be deleted as soon as possible after membership of the Association or engagement with the Association has ended but within four months after notification of the decision, unless consent has been given for longer data storage, or a requirement of local law

Specific information on account data

Affected data:	Data provided to administrate accounts
Processing purpose:	Setting up of accounts, administration of membership accounts
Categories of recipients:	Public authorities subject to priority legislation External service providers or other contractors. Other external bodies as far as the data subject has given their consent or a transmission of predominant interest is permitted.
Third-country transfers:	Contractors from outside the European Union may be used to fulfil and implement contracts.
Duration of data storage:	The duration of data storage depends on the duration of the existence of the account. After deleting the account all related data will also be deleted.

Specific information on data related to self-certifications

Affected data:	Data provided for self-certification
Processing purpose:	Implementation & administration of self-certifications
Categories of recipients:	Public authorities subject to priority legislation External service providers or other contractors. Other external bodies as far as the data subject has given their consent or a transmission of predominant interest is permitted.
Third-country transfers:	Contractors from outside the European Union may be used to fulfil and implement contracts.
Duration of data storage:	The duration of the data storage is for the life time of membership or the Association personnel are engaged with the Association unless impacted by local law

Specific information on data related to incident reports

Affected data:	Data provided in an incident report.
Processing purpose:	Addition of an incident to the incident database, administration of incidents
Categories of recipients:	Public authorities subject to priority legislation External service providers or other contractors. Other external bodies as far as the data subject has given their consent or a transmission of predominant interest is permitted.
Third-country transfers:	Contractors from outside the European Union may be used to fulfil and implement contracts.
Duration of data storage:	The duration of the data storage is for the life time of membership or the Association personnel are engaged with the Association unless impacted by local law

Additional information and contacts

In addition, you may invoke your rights to rectification or cancellation at any time, or to restrict the processing or exercise of your right to object to the processing and the right to data portability. Here you have the option to contact us via email to info@tapaemea.org. You also have the right to contact the data protection supervisory authority in case of any complaints.

A full list of TAPA EMEA General Data Protection Procedures can be downloaded using this link