Data protection policy

Policy prepared by:	Sander Dijkman
Approved by the board on:	May 15th 2016
Policy became operational on:	January 31st 2017
Next review date:	April 15th 2018

Introduction

ETPA B.V. needs to gather and use certain information about individuals.

They can include customers, suppliers, business contacts, employees and other pople the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

Why this policy exists

This data protection policy ensures ETPA B.V.:

- Complies with Dutch data protection law ("Wet Bescherming Persoonsgegevens") and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individual's data
- Protects itself from the risks of a data breach.

Data protection

The Wet Bescherming Persoonsgegevens (2001) describes how organisations – including ETPA – deals with processing personal data.

Personal data concerns all data with which a person can be identified with.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Within ETPA, the following principles must be adhered to:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date

5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area, unless that county or territory also ensures an adequate level of protection

Policy scope

This policy applies to all:

- ETPA entities
- all staff of ETPA
- All contractors, suppliers and other people working on behalf of ETPA.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside the WBP. This can include:

- Names of individuals (including Social Security Numbers)
- Postal addresses
- Email addresses
- IP addresses
- Telephone numbers

High risk personal data includes

- Copies of identification documentation
- Social Security Numbers
- EAN codes

Data protection risks

This policy helps to protect ETPA from data security risks, including:

- Breaches of confidentiality. i.e. information being given out inappropriately
- Failing to offer choice. i.e. all individuals should be free to choose how the company uses data relating to them
- Reputational damage. i.e. the company could suffer if hackers successfully gained access to sensitive data

Responsibilities

Everyone who works for or with ETPA has some responsibility for ensuring data is processed appropriately.

Data processing includes each activity related to personal data. This includes: collecting, documenting, sorting, storing, collating, updating, altering (including deleting), inspecting, appylying and distributing in any way including

Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The employees below have the following key responsibility:

- Board of directors is ultimately responsible for ensuring that ETPA meets its legal obligations
- Head of compliance is responsible for:
    - Keeping the directors updated about data protection responsibilities, risks and issues

    - Reviewing all data protection procedures and related policies annually.
    - Arranging data protection training and advice for the people covered by this policy
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data ETPA holds
    - Checking and approving contracts or agreements with third parties that may handle sensitive data
- IT manager is responsible for:
    - IT security policy
    - Ensuring all systems used for storing data meet acceptable security standarads
    - Performing regular checks and scans to ensure security of software
    - Evaluating third party services the company is considering to use to store or process data. i.e.
- Staff is responsible for:
    - Preventing that data used is only used for their work
    - Not sharing data informally
    - Taking sensible precautions i.e. as strong passwords and periodically resetting them
    - Half yearly review of data

Data storage

These rules describe how and where data should be safely stored. Questions about storing data can be directed to the head of compliance.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorized people can see them (clean desk policy)
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the ETPA's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data storage must adhere to the following terms:

Administration	**Term**
Financial administration including order and trade reporting	7 years
Personnel files	After end of employment period:

	7 years – salary slips and year statements 5 years – copy of passport 2 years – other
Mailings	2 years after de-rollment of the mailing

Personal data may only be stored if the purpose of use of that data is described and further processing may only be applied within the scope of that purpose.

Data accuracy

The law requires add to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort ETPA shall put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. These steps include:

- Holding data in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a participant's details when they call.
- ETPA will make it easy for data subjects to update the information ETPA holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Rights of persons involved

The WBP prescribes the following rights to those whose data is being processed:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.
Subject access requests from individuals should be made by email, addressed to ETPA at info@etpa.nl.

Disclosing data for other reasons

ETPA is required to disclose data to law enforcement agencies without consent of the data subject under certain circumstances. ETPA is however required to ensure whether the request is legitimate.

In the event of a serious data leak, the Board of Directors is required to report the leak to Autoriteit Persoonsgegevens. (https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0)

A data leak is considered serious when negative consequences to the subject are highly probable.

A data leak is defined as an instance where there is a security breach resulting in:

- Loss of personal data
- A likelihood of illegitimate processing of personal data

Instances of security breaches are: loss of USB stick, stolen laptop, unauthorized hack, malware or a calamity such as a fire.

Code of Conduct

3.4.6 Specific Rules of Conduct

4. Information Control

Employees frequently come into possession of information regarding not only ETPA, but also its participants and others doing business with ETPA and its participants. All Employees must observe the strictest confidentiality concerning all information entrusted to them by ETPA, whether relating to ETPA matters or relating to participant relationships that come to their attention in the course of their activities. Inadvertent or improper disclosure could be harmful to ETPA and its participants and may result in regulatory repercussions.

- Essential to the controlling of the flow of information within the Organisation, is the 'need to know' principle. This principle requires that information is only shared with those who have a legitimate business reason to receive such information. Prior to the communication of information, the existence of a 'need to know' basis must be established.

The obligation to safeguard information continues after termination of employment with ETPA. However, the obligation to maintain the confidentiality of information may be subject to legal or regulatory requirements to disclose that information. In such cases management should seek advice of local legal counsel to ascertain the legal obligation of disclosure.

Company Information
Employees may create, have access to or receive documents and information about ETPA ("Company Information"). Company Information may include, among other things, ETPA's intellectual property, business strategies and plans, marketing plans, financial data, operating budgets, staffing plans, employee lists, computer networks and participant information.

Protecting participant information whether related to the fact that a participant relationship exists or to individual transactions carried out by the participant, is important to ETPA and frequently required as a result of local privacy or data protection rules and standards. It does not matter whether the information regarding the participant is communicated on a personal basis by the participant or acquired in some other fashion in the exercise of professional activities.

- You must respect the privacy of participant information and ensure that the collection, use and transfer of such information complies with local privacy and data protection standards.

- Be cautious when handling participant information as its disclosure, intentional or otherwise, may restrict ETPA's ability to continue to work with the participant as it may create a conflict of interest

Inside Information
In some cases, Company Information qualifies as "inside information". As a general rule, inside information includes any non-public information about ETPA or its participants or other companies doing business with ETPA or its participants that (i) may have an effect on the price of an energy contract. ETPA services an anonymous orderbook. Until sufficient liquidity has been obtained on the exchange, orders and trades shall remain anonymous to participants.

Disclosure of inside information may only be made on a "need to know" basis. The misuse or unauthorized disclosure of inside information is a punishable offence, which may have legal

consequences for ETPA and any Employee concerned. Even the mere suspicion of insider trading may severely damage the ETPA's reputation.

- Avoid discussing inside information in places in or around the office where non-authorised Employees and/or external visitors may overhear you, such as the canteen, the lift, the parking place, corridors. Never discuss inside information in public places such as bars, restaurants, airports, or public transport.

ETPA expressly prohibits any form of exploitation of inside information.

In order to avoid any perception of possible insider trading, an Employee should not become a trader or partner in the business of a participant or a company related to a participant.

Information Handling
ETPA and its Employees must take all reasonable steps to preserve the confidentiality of information. For this reason, Company Information is in many cases classified. For example, documents or data classified as "confidential" may only be passed on to an Employee who has a legitimate "need to know" in connection with his or her work at ETPA or an individual who is authorized to receive such information (e.g. in response to a regulatory request). This is the case irrespective of the form in which the documents or data exist (in written/oral form, stored electronically/magnetically, etcetera). When dealing with classified documents and data, the specific handling instructions that apply must be observed at all times.

- Do not leave confidential or sensitive documents in places where others can read them. Documents which contain confidential information must not be left out in the open unattended and/or unsecured. Only discard of such confidential documents through a secure waste bin (e.g. a paper shredder).

When Employees leave ETPA they are obliged to surrender all Company Information and copies thereof that came into their possession in the course of the employment relationship to the Organisation.

- You must maintain strict confidentiality concerning all information that you create, have access to, or receive in the course of your employment with ETPA.

IT Security Policy

6.3.5 Protection in relation to safeguarding Participant data

Data comes in many forms; sales lists, contact databases, company processes, client work, performance reports, financial records, orders, trades, transactions, internal company records, HR information and payroll details.

Within ETPA we consider the orders, trades and transactions to have the highest risk and therefore warrants the highest security.

Responsibility
Order, trade and transaction data shall only be managed by the following system users: monitoring, support and compliance. System users and system administrators are separate functions.

Devices
Order, trade and transaction data shall only be managed on devices for which:

- Up-to-date anti-virus programs are in place
- effective patch management systems are in place for PCs and servers
- a segmented network is implemented
- All devices and applications shall be equipped with login and password verification

No USB storage devices without password security

Environment
The environment related to orders, trades and transaction data shall be subject to

- Regular systems vulnerability scan
- System access and events (printing, file saves USB plug-ins) logging
- Impact due to outsourcing
- Monitoring should evaluate the whole security system of the firm. The system should be an overview of user activity (logon/off, remote access, USB read/writes, file prints, website access). The overview should be monitored regularly for abnormal activity by staff that is able to interpret the data (unexpected network ports, services, applications).

Response & recovery

ETPA shall ensure that the response to an event is pre-planned, and practiced and covered in the operational risk process.

These areas are controlled by the COO function, including updates on the recovery process to the compliance department.

Response time is set at 6 hours.

Training

Employees shall be trained annually on IT security risk and measures because human intervention is often the weakest link.