Data Privacy & Breach Policy

boxx
global expat solutions

Content

Data Privacy & Breach Policy

A. Data Privacy Policy

1. Purpose of this policy

Boxx needs personal data to be able to perform services for our clients and their employees. For every service (relocation (coordination), immigration, HR, tax) personal data (and lots of it) is needed to do our job.

The purpose of this policy is to outline the approach Boxx takes towards personal data and ensuring the protection thereof. This policy describes how personal data must be collected, handled, and stored to meet the Boxx' data protection standards and any legal requirements.

In the event a data protection breach should occur, part B of this policy outlines our approach and steps that will be taken to resolve the breach and prevent a breach from happening again.

This policy will be reviewed annually in January of each year. The policy is written for all Boxx employees, management, service providers, contractors and third parties that have access to information of Boxx' corporate and individual clients.

2. Types of data

This policy relates to all kinds of personal data. Examples of personal data that Boxx uses to provide services are, but are not limited to:

- First name
- Last name
- Gender
- Copy passport
- Employee number
- (Tax and/or social security) registration number
- Date of birth
- Nationality
- Address
- Email address
- Phone number
- Marital status and family composition
- Data of family members
- Marital- and/or birth certificate
- Remuneration details and pay slips
- Employment information (position, start date, end date)
- Employment and/or assignment contract
- Work and/or resident permit and visa

- Travel details
- Tax returns and information needed for the tax return (bank details, information on deductions etc.)
- Passport photographs

3. Data Privacy Consent

Every individual client will need to sign a Data Privacy Consent Form before Boxx can process personal data on behalf of the individual and his/her family members. The Data Privacy Consent Form will be provided digitally via the personal portal of the individual client in Boxx' customer portal: www.MyBoxx.World.

4. Data Processor Agreement

Boxx will enter into Data Processor Agreements with all corporate clients.

5. Data storage

Boxx stores client data electronically in a secure way and data is only accessible by Boxx employees who will need it for their work. The data can only be accessed by way of two-step authentication (password and one-time password). The data is kept in a secure cloud environment or protected by two separate firewalls. Boxx employees are not allowed to store client data on removable media. Back ups of data are made daily and kept for 31 days.

When data is stored on paper (or electronically kept and printed for use), it is kept in a secure place where unauthorised people cannot access it. After use, prints or notes on paper are disposed in a secure way (shredded).

6. Data usage and disclosure

When personal data is accessed by Boxx employees and used to provide the services to our clients, it is handled with great care. Boxx employees always lock the screens of their computer when away from their desk. If unlocked and not used, computers will automatically lock.

Personal data will not be shared by email, as this form of communication is not secure, other than replying to a message containing personal data sent by the individual client himself or herself to Boxx. Boxx employees are not allowed to save personal data on their own computer and should always access and update the centrally stored copy of any data.

7. Data accuracy

It is the responsibility of all Boxx employees who work with the personal data to take steps to ensure it is kept as accurate and up to date as possible. Data will be held in as few places as necessary. Every opportunity will be taken to ensure data is updated. For instance, by confirming a client's details during a call about the services to provide. Data will be updated as soon as inaccuracies are discovered (e.g. after receiving a failure message on an email address).

Clients can provide changes in personal data in a secure way via the Boxx customer portal: www.MyBoxx.World.

8. Employee training

Boxx employees are trained on data privacy and protection on an ongoing basis, with at least one mandatory class room training per year.

9. Boxx' partner network: Frame

Boxx undertakes to ensure that partner companies authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10. Storage term and deleting information

Boxx will delete all personal data after a period of 7 years has expired after the end of service delivery for the individual client. Upon request of an individual client personal data is deleted immediately, unless the law prohibits this. In that case we will inform the client of our legal obligations.

B. Data Privacy Breach Policy

1. Data privacy breach - general

A data breach generally refers to the unauthorised access and retrieval of information that may include corporate and personal data. Managing data breaches is important to protect the personal data of our clients and their employees when a data breach occurs.

2. How data breaches could occur

Data breaches can occur for different reasons. They may be caused by employees, parties external to the organisation or computer system errors. Possible ways in which a data breach may occur, and Boxx employees should be thoroughly aware of, are:

- Human error:
  - Loss of laptop, phone, data storage devices or paper records containing client and/or personal data;
  - Sending client and/or personal data to a wrong e-mail or physical address, or disclosing data to a wrong recipient;
  - Unauthorised access or disclosure of client and/or personal data by employees;
  - Improper disposal of client and/or personal data (e.g. hard disk, storage media or paper documents containing client and/or personal data sold or discarded before data is properly deleted);
- Malicious activities:
  - Hacking incidents / illegal access to databases containing client and/or personal data;
  - Theft of laptop, phone, data storage devices or paper records containing client and/or personal data;
  - Scams that trick organisations into releasing client and/or personal data;
- Computer system error:
  - Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to personal data stored on computer systems.

3. Data Breach Management Plan

It is the policy of Boxx that in the event that a data breach happens,
the following breach management plan is strictly adhered to. There are five steps to this Breach Management Plan:

I. Identification and classification
II. Containment and recovery
III. Risk assessment
IV. Reporting of breach
V. Evaluation of the response & recovery to prevent future breaches

I. Identification and classification

When a data breach occurs, this should be immediately reported by sending a Data Breach Incident Report to:

GDPR@boxx-expat.com

A copy of the report should be sent to

- the ICT team - ICT@boxx-expat.com
- the Client Account Manager
- If applicable, the employee's line manager

The report should include:

- Details of the breach, such as:
  - Date;
  - Time;
  - Who/what reported the breach;
  - Description of the breach;
  - Details of any ICT systems involved;
    Corroborating material such as error messages, log files, etc.
- An account of immediate actions taken;
- An account of the Breach Management steps (II – V) to be taken.

II. Containment and recovery

As part of the Breach Management steps to be taken, the following measures have to be considered immediately, where applicable:

- Shut down the compromised system that led to the data breach;
- Prevent further unauthorised access to the system;
- Reset passwords if accounts and passwords have been compromised;
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach (e.g. remotely disabling a lost laptop containing personal data of clients and/or individuals);
- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system;

- Notify the police if criminal activity is suspected and preserve evidence for investigation (e.g. hacking, theft or unauthorised system access by an employee);
- Put a stop to practices that led to the data breach;
- Address lapses in processes that led to the data breach.

III. Risk assessment

Knowing the risks and impact of the data breach will help to determine the consequences to affected organisations and individuals, as well as the steps necessary to notify the organisations and individuals affected. For each data breach it has to be assessed:

- How many people were affected?
- Whose personal data has been breached?
- To whom does the personal data belong? (e.g. clients, their employees, Boxx employees, contractors, vendors or other third parties)
- What types of personal data were involved?
- Is there a risk to reputation, identity theft, safety and/or financial loss of affected organisations/individuals?
- How sensitive is the information?
- Do any additional measures have to be put in place to minimise the impact of the data breach?
- What caused the data breach?
- When and how often did the breach occur?
- Who might gain access to the compromised personal data?
- Will compromised data affect transactions with any other third parties?
- Who needs to be notified?

IV. Reporting of breach

Clients and/or individuals affected by the data breach should be notified.

Who to notify -

- We will notify organisations and/or individuals whose personal data have been compromised;
- We will notify other third parties such as banks, credit card companies or the police, where relevant;

When to Notify -

- We notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data;

- We notify affected organisations and/or individuals when the data breach is resolved;

How to Notify -

- We will reach out to affected organisations and/or individuals in the most effective way, taking into consideration the urgency of the situation and number of individuals affected (e.g. e-mails, telephone calls, letters);
- Notifications will be simple to understand, specific and provide clear instructions on what individuals can do to protect themselves;

What to Notify -

- How and when the data breach occurred, types of personal data involved in the data breach;
- What Boxx has done or will be doing in response to the risks brought about by the data breach;
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused;
- Contact details and how affected individuals can reach Boxx for further information or assistance.

V. Evaluation of the response & recovery to prevent future breaches

After these steps have been taken to resolve the data breach, the cause of the breach has to be reviewed and it has to be evaluated whether existing protection and prevention measures are sufficient to prevent similar breaches from occurring.

We will assess whether:

- Audits were regularly conducted on both physical and IT-related security measures;
- There are processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse;
- There were weaknesses in existing security measures and protection measures, or weaknesses in the use of portable storage devices or connectivity to the Internet;
- The methods for accessing and transmitting personal data were sufficiently secure;
- Support services from external parties should be enhanced, such as vendors and partners;
- The responsibilities of vendors and partners is clearly defined in relation to the handling of personal data;
- There is a need to develop new data-breach scenarios;
- There were enough resources to manage the data breach;
- Key personnel were given sufficient resources to manage the incident;
- Employees were aware of security related issues;

- Training was provided on personal data protection matters and incident management skills;
- Employees were informed of the data breach and the learning points from the incident;
- Management was involved in the management of the data breach;
- There was a clear line of responsibility and communication during the management of the data breach.

For any questions on this Policy – please send your questions to: GDPR@boxx-expat.com