Data protection policy Global Alliance for Banking on Values - GABV

Context and overview

Key details

- Policy prepared by: Global Alliance for Banking on Values
- Approved by board / management on: 21/05/2018
- Policy became operational on: 25/05/2018

Introduction

The Global Alliance for Banking on Values - GABV needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people 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 that the Global Alliance for Banking on Values - GABV:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including the Global Alliance for Banking on Values - GABV — must collect, handle and store personal information.

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.

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of the Global Alliance for Banking on Values - GABV
- All staff and volunteers of the Global Alliance for Banking on Values - GABV
- All contractors, suppliers and other people working on behalf of the Global Alliance for Banking on Values - GABV

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect the Global Alliance for Banking on Values - GABV from some very real data security risks, including:

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

How we use your personal data

We may process data about your use of our website and services ("usage data"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. This usage data may be processed for the purposes of analysing the use of the website and improve it. The legal basis for this processing are our legitimate interests as per Article 6(1) lit. f GDPR.

We may process your account data ("account data"). The account data may include your name, email address, list of merchants you want to be updated about new coupons for. The source of the account data is you. The account data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is consent as per Art. 6(1) lit. a GDPR.

International transfers of your personal data

The hosting facilities for our website and some service providers we use are situated in countries outside the European Economic Area. Transfers to each of these countries will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission.

Cookies used by our service providers

Our service providers use cookies and those cookies may be stored on your computer when you visit our website.

We use Google Analytics (with the anonymizer function enabled) to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: https://www.google.com/policies/privacy/. Google is certified under the Privacy Shield Framework thus offers a guarantee to follow EU regulation concerning the protection of personal data.

General staff guidelines

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **The Global Alliance for Banking on Values - GABV will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the marketing coordinator.

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

Data accuracy

The law requires the Global Alliance for Banking on Values - GABV 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 the Global Alliance for Banking on Values - GABV should 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.

Subject access requests

All individuals who are the subject of personal data held by Global Alliance for Banking on Values - GABV are entitled to:

- 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 the data controller at admin@gabv.org. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the Global Alliance for Banking on Values - GABV will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Our details

This website is owned and operated by the Global Alliance for Banking on Values.

We are registered in the Netherlands, being our office and principal place of business are at Global Alliance for Banking on Values, Nieuweroordweg 1, P.O. Box 55, 3700 AB Zeist, The Netherlands.

You can contact us:

(a) by post, to the postal address given above;

(b) using our website contact form;

(c) by telephone, on +31(0)30 694 3062

(d) by email, using admin@gabv.org.