



Customer relationship made easy

Take a Byte Limited

Data Protection Policy

Document

© 2018 Take A Byte Limited.

Last updated 21st February 2018

For all enquiries about the content of this document please email enquiries1@takeabyte.co.uk.

Table of Contents

| | |
|--|-----------|
| Introduction | 4 |
| Definitions | 4 |
| Scope | 5 |
| Our procedures | 5 |
| Subject access requests | 8 |
| GDPR provisions | 9 |
| Right to be forgotten | 10 |
| Privacy by design and default | 10 |
| International data transfers | 10 |
| Data audit and register | 11 |
| Consequences of failing to comply | 11 |
| GDPR with regard to Take A Bytes own Customers data | 12 |

Introduction

We hold personal data about our employees, clients, suppliers and other individuals for the sole purpose of supplying a customer relationship management system to our customers.

We also hold large amounts of personal data on behalf of our customers who entrust its safety and security to us.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

| | |
|--------------------------|--|
| Business purposes | <p>The purposes for which personal data may be used by us:</p> <p>Personnel, administrative, financial, regulatory, payroll and business development purposes.</p> <p><i>Business purposes include the following:</i></p> <ul style="list-style-type: none">- <i>Compliance with our legal, regulatory and corporate governance obligations and good practice</i>- <i>Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests</i>- <i>Ensuring business policies are adhered to (such as policies covering email and internet use)</i>- <i>Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking</i>- <i>Investigating complaints</i>- <i>Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments</i>- <i>Monitoring staff conduct, disciplinary matters</i>- <i>Marketing our business</i> |
|--------------------------|--|

| | |
|-------------------------|--|
| Personal data | Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. <i>Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.</i> |
| Sensitive personal data | <i>Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.</i> |

Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our Data Protection Officer, Damien Bhanji has overall responsibility for the day-to-day implementation of this policy.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officers responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Take A Byte Limited.
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy

- In most cases this provision will apply to routine business data processing activities.

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed

- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer.

Subject access requests

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the DPO. We may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

GDPR provisions

Where not specified previously in this policy, all the provisions in this document will be in effect on or before 25 May 2018.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers

No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

GDPR with regard to Take A Bytes own Customers data

Take A Byte holds personal data on behalf of its customers in order for them to run their own businesses. This section details what Take A Byte supplies with regard to data protection of Take A Byte customers own personal data.

Security

Take A Byte ensures that all customer data is accessed in a secure manner using encrypted communications so that personal data cannot be intercepted by third parties.

Storage of all data is only on secure servers that are kept up to date with the latest security software.

Location

All data is stored strictly within the UK. The 4 locations used are London, Chelmsford, Coventry and Gosport.

Data theft

In the event that any customer data is stolen from Take A Byte then the customer or customers affected will be notified within 7 days of the theft.

Tools to help with GDPR compliance

It is up to each customer of Take A Byte to ensure that they are GDPR compliant. To assist with this Take A Byte will supply technical tools to its customers to make this process as easy as possible.

Seeking permission from existing customers

For customers that are already on the database permission must be requested to retain their personal data. The 'In-Contact' system will provide a method of contacting existing customers using the 'mailshot' feature already built into 'In-Contact'. A special form of stationery will be used with voting buttons embedded in the email. This will allow your own customers to quickly respond with either 'Yes, I'm happy for you to retain my data' or

'No, I want you to remove my data'. The use of these buttons will mean your own staff will not need to process the responses thus speeding up the process and improving accuracy.

Customer Data Retention

When a booking is taken the customer will be asked if their details can be held on the database and for how long. They will also be asked if their details can be passed on to other companies for the purpose of marketing. Both questions will be 'opt in', that is the default will be 'no'. These questions will be asked each time a booking is made.

The right to be forgotten

When receiving a request to have a customer's data removed a record of the request will be stored before all personal data is removed. This will allow 'Take A Byte' customers to demonstrate that they are complying by showing this log to any investigating authority. The 'In-Contact' system will ensure that all personal data is securely erased.

The right to see a copy of all personal information

When receiving a request to see all personal information the 'In-Contact' system will create a document containing the personal information and send it to the customer. If the information is emailed then a portable version of the personal information will be attached. A log of the request will be kept so that compliance can be verified to any investigating authority.

GDPR Compliance Report

The compliance report will show you how many of the contacts on your database meet compliance requirements and how many do not. This will then allow you to take appropriate action to improve your own compliance, for example, by secure erasing those that are not compliant.