ByBox | Policies

Data Protection Policy & Procedure for Customer and Third Party Data

Issue no. 3
June 2016

Contents

1. Introduction

The Data Protection Act 1998 ("the Act"; "the DPA") governs the handling of all personal data by ByBox. Personal data is information in any format which relates to an identifiable living individual.

ByBox is committed as a matter of policy to complying with its obligations under the Act in order to protect the personal privacy of all individuals whose data we hold. This policy, together with our Data Security Policy, sets out how ByBox will comply with these obligations when handling personal data relating to ByBox's customers. Following this policy will help ensure that the handling of all personal data by ByBox complies with the DPA.

ByBox's policy in relation to the handling of staff data is set out in the ByBox "Staff Data Protection Policy"

When we handle personal data under contract with our business customers (e.g. delivery details that are passed to us by business customers), legal responsibility for data protection compliance rests with our customers rather than with us. For this data, our primary obligation is to follow our customers' instructions. But it is important to bear in mind that all our business customers expect us to ensure that personal data relating to their customers is handled by us securely and with proper regard for the privacy of their own customers. Compliance with this policy will help ensure that all personal data held by ByBox is handled in accordance with the law.

All ByBox Staff are required to comply with this Policy, which should be read together with the Information Security Policy [and any other relevant information governance policy].

Compliance with this policy is a condition of employment and any deliberate breach of this policy will result in disciplinary action, which may include dismissal and possible prosecution.

2. Eight Data Protection Principles

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal Data shall be obtained and processed only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal Data shall be adequate, relevant and not excessive in relation to the purposes or purpose for which they are processed.
- Personal Data shall be accurate and where necessary kept up to date.
- Personal Data shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal Data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Personal Data shall not be transferred to a country or territory outside the European Economic Area unless there is an adequate level of data protection in that country.

In order to comply with these principles ByBox will:

- ensure personal data is used fairly and only in accordance with the expectations of affected individuals
- meet its legal obligations to specify the purposes for which personal data will be used, by including relevant information within its on---line privacy policy and on the face of any paper based data collection forms.
- collect and process personal information only to the extent necessary for operational purposes or to comply with legal requirements.
- take reasonable steps to ensure that personal data is accurate and up to date.
- retain personal data only for so long as this is necessary having regard to legitimate operational need and the expectations of individuals concerned.
- ensure that individual customers whose data is held by ByBox are able to exercise their rights under the Act, particularly their rights to request copies of their personal data
- take appropriate technical and organisational security measures to safeguard personal information as set out in the Information Security Policy.
- ensure that any contractors engaged to handle personal data on our behalf are properly supervised and are subject to appropriate contractual controls
- provide all staff who are involved in handling personal data with appropriate and relevant training
- ensure that personal information is not transferred to a country outside Europe without suitable safeguards.
- audit data security and compliance with this policy on a periodic basis.

3. Purposes for Which Personal Data are Held

Data relating to individual users of ByBox services is held by ByBox for the purpose of service delivery, invoicing, product and business development. ByBox will not use its customer data for other unrelated purposes without consent unless required to do so by law. Customers are made aware about the intended use of their data by means of our on line privacy statement and our entry on the Information Commissioner's Register of data controllers (registration number: Z815832X).

4. Sensitive Personal Data

Sensitive personal data includes information relating to the following matters:

Information as to a person's

- racial or ethnic origin.

- political opinions.
- religious or similar beliefs.
- trade union membership.
- physical or mental health or condition.
- sexual life.
- The commission or alleged commission of any offence
- The outcome of any prosecution

ByBox does not normally hold sensitive personal data relating to customers. However, personal data falling within these categories is subject to additional protection under the Act and, therefore, where sensitive data is collected for any reason, it is usually necessary to obtain specific consent from the individuals concerned. Very considerable care should be taken to ensure such data is handled securely.

5. Responsibility for the Processing of Personal Data

The Chief Executive is responsible for ensuring that the organisation complies with the DPA.

All employees who have access to personal data are responsible for complying with this policy and with other relevant policies and procedures relating to data handling. Failure to comply with these policies and procedures may result in disciplinary action up to and including summary dismissal.

6. Data Quality

Under the DPA ByBox is required to ensure that personal data are

- relevant, adequate and not excessive
- accurate and up to date
- not held for longer than is necessary

Complying with these obligations makes good business sense and is important to protect individual privacy. ByBox will therefore review periodically the customer data it collects in order to ensure that this data is adequate and relevant to the services we provide and is not excessive. We will also make it easy for our customers to let us know of any change in their circumstances so that we can update our records accordingly. All information will be disposed of securely when no longer required in accordance with our records disposal schedule.

7. Disclosure of Personal Data

ByBox will not usually disclose personal data relating to its customers to third parties unless the customer has consented to the disclosure. In exceptional circumstances the DPA does permit personal data to be disclosed to third parties without consent. Examples include disclosures to statutory bodies for the purpose of detecting crime, fraud or money laundering or disclosures necessary for medical purposes. In the case of personal data relating to clients of our business customers, this should never disclosed to any third party unless this is specifically authorised by our business customers.

If, exceptionally, it is necessary to disclose personal data to third parties, ByBox will ensure that this is done securely and in a manner that minimises privacy risks.

8. Access to Personal Data ("Subject Access Requests")

Individuals have the legal right to request the disclosure of personal data relating to them that is held by ByBox. ByBox is entitled to charge a fee of £10. However, we may exercise discretion when considering whether a fee should be charged. Anyone seeking to make a subject access request should be asked to supply evidence of their identity and make their request in writing. Where a subject access request is submitted to us, a full response should be issued within 40 days. There are some exemptions from the duty to supply information, especially where disclosure will involve the disclosure of information about other people. If there are any concerns about the disclosure of information in response to a request, advice should be sought.

9. Data Security

Information Security is a matter of priority for ByBox as our customers rely on us to look after their personal information. In addition organisations that fail to have proper data security arrangements in place are liable to fines of up to £500,000.

Data security includes IT and physical security but also refers to the systems, policies and procedures that are necessary in order to guard against loss, damage, destruction of personal data and against inappropriate or unlawful access. All staff are expected to comply with the Data Security Policy when handling personal data.

Data security depends very considerably on staff training and awareness. ByBox is committed to ensuring that all staff with data handling responsibilities receives appropriate training in relation to data security and confidentiality.

ByBox recognises that the use of external contractors to handle personal data usually creates additional data security risks and acknowledges that it is a specific requirement of the DPA that any contractors that are engaged to handle personal data on our behalf must be carefully selected and properly supervised. Therefore, whenever a contractor is engaged to carry out work that involves the processing of personal data, ByBox will allow the contactor to handle personal data only if we are satisfied that the contractor's data security measures are adequate and only where a written contract setting out the contractor's obligations in relation to that data are clearly set out in accordance with the DPA's requirements.

10. Data Security Breaches

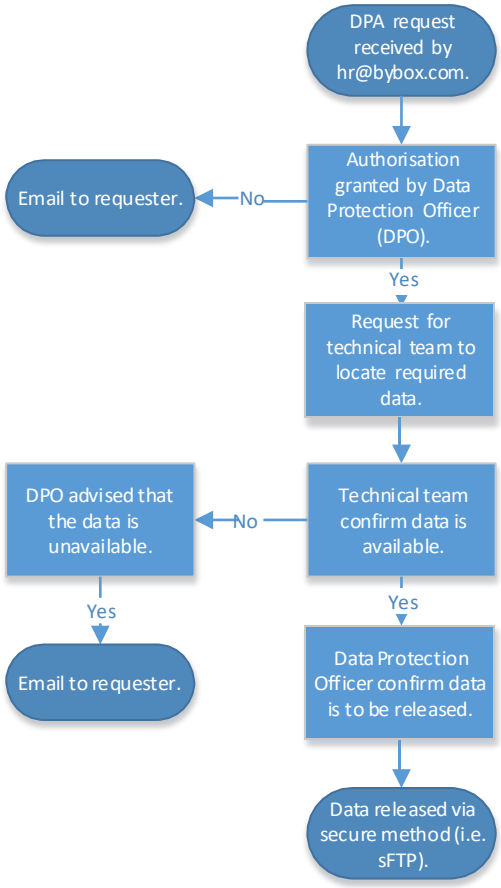
Any data security breach should be reported to the Director of Security so that action can be taken to protect affected individuals and to ensure that lessons are learned to minimise the risk of recurrence.

11. Requesting Data

On completion of the form below. Please forward to the following e---mail address HR@bybox.com. Where your request will be action accordingly and you will be kept informed of your requests is progressing.

12. Data Release Process

Any request for data will be subject to the following release process:



REQUEST FOR DISCLOSURE OF INFORMATION UNDER THE

DATA PROTECTION ACT 1998 SECTION 29(3)

Applicant Details	
Name of Applicant:	
Address of Applicant:	
Email address:	
Telephone:	

Where Applicable	
Company Name:	
Department Name:	
Company Address:	

Nature of Enquiry		
Reason for Request	Without it, the prevention or detection of crime will be prejudiced	Yes / No
	Without it, the apprehension or prosecution of offenders will be prejudiced	Yes / No
	Other, please specify:	
Location:		
Date and Time:		
Subject Name (if applicable):		

Required Information:	

Declaration --- If we do not receive the data, this will prejudice the purpose(s) specified above. We accept that the data supplied is governed by the Data Protection Act 1998. We agree to use only the data for the purpose(s) specified above, and in accordance with the Act and treat the data in confidence.

All data should be handled in accordance with local Data Protection Laws

Please complete this section if information is being requested by a company on behalf of a Third Party

Authorisation (to be completed by an authorised person)	
Name:	
Title:	
Date:	
Signature:	
Email address:	
Telephone:	