box-it
documents are our business

Box-it data processor statement of compliance and contract addendum

May 2018

1 Introduction

The EU's General Data Protection Regulation (EU) 2016/679 (GDPR) will come into force on 25 May 2018, this will supersede the Data Protection Act of 1998. Whilst certain existing provisions will remain the same, the GDPR introduces new and additional data protection obligations on companies handling personal data.

Box-it has entered into one or more agreements with you for the provision of one or more of the following services:

- paper and digital records management and related services, including: cataloguing, indexing, digitisation
- collection, storage and retrieval of archived records
- end-of-life secure document destruction.

In providing such services to you, this means we are collecting and processing personal data belonging to or provided by your organisation, on your behalf.

Where processing is to be carried out on behalf of a controller (you by us) the GDPR requires a written contract to be in place *(GDPR Article 28(3))* with certain minimum terms.

This statement of compliance sets out how the Box-it group of companies, hereafter referred to as Box-it, complies with our obligations under the GDPR in our role as *data processor* on behalf of you, *the data controller* (our Client).

This statement of compliance must be read in conjunction with the Box-it contracted terms and conditions and any GDPR-related variations you have provided to us. These all form part of the processing agreement between you (the data controller) and Box-it (the data processor).

Please refer to *Appendix* A for the definitions and interpretation of the terms referenced in this statement.

2 Scope, nature and purpose of processing

The scope of this statement of compliance applies to Box-it's obligations when processing personal data on behalf of you, the data controller (our client), in the delivery of the products and services as detailed in your Box-it *Schedule of services*. These include one or more of the following:

- paper and digital records management and related services, including: cataloguing, indexing, digitisation
- collection, storage and retrieval of archived records
- end-of-life secure document destruction.

This statement of compliance references some data controller responsibilities and assumes that as data controller you are fulfilling your obligations under GDPR accordingly.

3 Duration of processing

We will process your personal data for the duration of your contract, until such a time that your contract is terminated, or for the period required by applicable law or statutory limitation periods, whichever is greater.

Please refer to your contract and *Schedule of services* for further details of the term of your contract.

4 Data processing

4.1 Types of personal data to be processed

Box-it may process the following categories of personal data on behalf of its data controllers. personal details (name, title, marital status, qualifications, date of birth, identity number, passport number, national insurance number, NHS number)

- contact details (telephone numbers, email addresses, fax number, social media names, address)
- HR data
- system access, usage, authorisation data
- financial data
- legal data
- government records
- other records containing personal data.

Please note: the above list is indicative of the type of data that we process, it is not exhaustive.

Box-it may also process the following **special categories** of personal data:

- health and medical records
- ethnicity
- criminal records and convictions
- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning a natural person's sex life or sexual orientation
- data relating to criminal convictions and offences.

4.2 Categories of data subjects

Box-it may process the following categories of data subjects on behalf of its data controllers:

- the client's employees (including temporary workers, volunteers, trainees, pre-hires, applicants)
- the client's (potential and actual) customers
- the client's business partners
- employees of the client's business partners
- the client's visitors
- the client's suppliers
- the client's subcontractors
- employees of the client's suppliers or subcontractors.

4.3 Data retention

The data controller is responsible for maintaining and managing the retention periods against all relevant data stored on its behalf by Box-it as data processor. The data controller will instruct Box-it to destroy data as and when required, in accordance with the data controller's retention schedules.

The data processor will ensure that data is securely destroyed, as instructed by the data controller.

5 Data processor obligations

Box-it will process your personal data in accordance with our obligations under *Article 28* of the GDPR as set out below.

5.1 Processing personal data

Box-it will:

5.1.1	Process your personal data for the sole purpose of providing the services set out in your *schedule of services* and in accordance with your written instructions, or as is required by law or any supervisory authority.
5.1.2	Process the personal data only on documented instructions from you, including with regard to transfers of personal data in or to countries outside the European Economic Area (EEA) or to any international organisation with your prior written consent, unless required otherwise to comply with any EEA or member state law (in which case, you shall provide prior notice to Box-it of such legal requirement, unless that law prohibits this disclosure on important grounds of public interest).
5.1.3	Not (unless otherwise permitted in accordance with the terms of the contract) engage another processor in carrying out any processing activities in respect of the personal data without the prior specific or general written consent of the data controller (such authorisation not to be unreasonably withheld, conditioned or delayed). Box-it will inform the data controller of any intended changes concerning the addition or replacement of other processors, thereby giving the data controller the opportunity to object to such changes. Box-it will appoint such processors under a written contract containing materially the same obligations as set out in this statement of compliance.
5.1.4	At your written request, ensure that without delay, and in line with the contract, all personal data is either securely deleted or securely returned to you in such form as you reasonably request after the earlier of: • the termination of the contract for the provision of the relevant services related to processing of such personal data or • when processing by Box-it of any personal data is no longer required for the purpose of Box-it's performance of its relevant obligations under the contract. And securely delete existing copies (except to the extent that storage of any such data is required by applicable law).

5.2 General technical and organisational information security measures

Box-it will:

5.2.1	Box-it will take appropriate technical and organisational security measures against unauthorised or unlawful processing of personal data such as accidental or unlawful loss, alteration, unauthorised disclosure or access, damage or destruction of personal data in accordance with the GDPR *articles 28* and *32*. All of this is validated through our certified ISO 27001 Information Security Management System, a copy of which is available at: https://www.boxit.co.uk/company/iso-standards/270012013-information-security/
5.2.2	Ensure that persons authorised on behalf of Box-it and its subcontractors to process such personal data are committed to contractually binding confidentiality commitments or are subject to a statutory obligation of confidentiality.

5.3 Assisting the data controller

Box-it will:

5.3.1	Give information and reasonable assistance to the data controller (including by taking all appropriate technical and organisational measures) to enable it to respond within required timescales to a request made by a data subject to exercise his or her rights under *Chapter III* of the GDPR (and any similar obligations under applicable data protection laws) in relation to personal data processed by Box-it on behalf of the data controller (the client).
5.3.2	Assist the data controller in ensuring compliance with the obligations pursuant to *Articles 32* to *36* of the GDPR, taking into account the nature of processing and the information available to Box-it.
5.3.3	Promptly notify the data controller if it becomes aware of any personal data breach that involves personal data processed by Box-it on behalf of the data controller.
5.3.4	Provide such information, co-operation and other assistance (taking into account the nature of processing and the information available to Box-it) to assist the data controller in its obligations under GDPR including with respect to: • security of processing • assistance to notify personal data breaches to the relevant supervisory authority • assistance to advise data subjects when there has been a personal data breach • taking all reasonable steps to address such a personal data breach, including, where appropriate, measures to mitigate its possible adverse effects and will consult with the data controller in respect of such resolution or mitigation • data protection impact assessments (as defined in GDPR) • consulting with the relevant supervisory authority regarding high risk processing.
5.3.5	Record and promptly refer all requests, communications and complaints to the data controller which relate (or which may relate) to any personal data. Box-it will not respond to any without the data controller's express written approval and strictly in accordance with the data controller's instructions, unless legally prohibited.

5.4 Compliance obligations

Box-it will:

5.4.1	Promptly make available to you such information as is reasonably required to demonstrate Box-it's and the data controller's compliance with our respective obligations under this statement of compliance and the GDPR, and allow for, permit and contribute to audits, including inspections, by you (or another auditor mandated by you) for this purpose at your request from time to time. Box-it will provide access to all relevant premises, systems, personnel and records during normal business hours (09:00- 17:00) for the purposes of each such audit or inspection upon reasonable prior notice and provide and procure all further reasonable co-operation, access and assistance in relation to any such audit or inspection.

6 Declaration

6.1 Box-it declaration *(the data processor)*

This statement of compliance clearly sets out Box-it's obligations and provisions under GDPR when acting on your behalf as a data processor. It forms an integral part of the legal basis of our relationship with you.

These obligations and provisions are monitored for their continued suitability and adequacy for compliance with GDPR. They are also audited by our Data Protection Officer to ensure that they are adhered to.

James Mair
Managing Director Box-it South East
18 May 2018

Appendix A – Definitions and interpretation

GDPR term	Definition
Data	Any information which is stored electronically or on paper.
Data controller	The individual or organisations who control and are responsible for determining the purpose, the keeping and use of data.
Data processor	A person, public authority, agency or other body which processes personal data on behalf of the controller. Examples of processing personal data: - staff management and payroll administration - databases containing personal data - sending direct marketing emails - CCTV
Data protection laws	Any applicable law relating to the processing, privacy and use of personal data, as applicable to either party or to the services including: - the GDPR - any laws that replace, extend, re-enact, consolidate or amend any of the foregoing - all guidance, guidelines, codes of practice and codes of conduct issued by any relevant supervisory authority relating to such applicable laws (in each case whether or not legally binding).
Data subjects	An individual to whom the personal data relates.
Data users	Staff, suppliers, third parties or any other interested parties whose work involves using personal data. Data users have a duty to protect the information they handle by following the Company's data protection and information security policies at all times.
International organisation	Has the meaning given in applicable data protection laws.
Member state	Any relevant member state of the European Union (EU) or European Economic Area (EEA).
Personal data	Information relating to an identified or identifiable natural person. This includes: - personal contact information - criminal convictions - financial information - driving licence number - passport information - education and training - employment details - performance management information - IP or email addresses, mobile device IDs.
Processing	Has the meaning given in applicable data protection laws. Related expressions, including 'process', 'processed' and 'processes' shall be construed accordingly.
Schedule of services	The agreed products and services to be delivered by Box-it under your Box-it contract and terms and conditions, and the agreed prices.
Sensitive personal data (*special categories and criminal convictions data*)	Personal data in relation to fundamental rights and freedoms merit specific protection because the context of their processing could create significant risks to the fundamental rights and freedoms of individuals. These include: - racial or ethnic origin - political opinions

	- information on religion or philosophical beliefs - trade union membership - genetic or health status, including physical or mental health or conditions - sexual orientation or sex life - biometric data - alleged criminal offences or criminal convictions.
Services	All services provided by Box-it under your Box-it contract, terms and conditions, schedule of services and any other related contractual agreements.
Supervisory authority	Any regulator, authority or body responsible for administering data protection laws.