

## DATA SECURITY POLICY

### 1. INTRODUCTION

#### 1.1 PURPOSE OF POLICY

This Data Security Policy ("**Policy**") sets out how Stauff Anglia Limited ("**we**", "**our**", "**us**", "**the Company**", "**Stauff**") handles the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Policy applies to all Company Personnel ("**you**", "**your**"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and you must attend any training on its requirements, which will be provided by the Data Protection Manager ("**DPM**"). This Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

#### 1.2 DEFINITIONS

In this Policy, the following terms shall have the following meanings:

**Company Personnel:** all employees, workers, contractors, agency workers, consultants, directors, members and others;

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them;

**Data Controller:** the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes;

**Data Subject:** a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and will have legal rights regarding their Personal Data;

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway;

**Explicit Consent:** consent which requires a very clear and specific statement (i.e., not just action);

**General Data Protection Regulation (GDPR):** the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR;

**Personal Data:** any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour;

**Personal Data Breach:** any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach;

**Processing or Process:** any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties;

**Pseudonymisation or Pseudonymised:** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure;

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

## 2. SCOPE

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in our organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

Everybody within Stauff is responsible for ensuring all Company Personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPM is responsible for overseeing this Policy. This post is held by [INSERT NAME].

Please contact the DPM with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed.

### **3. PERSONAL DATA PROTECTION PRINCIPLES**

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- (a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- (b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- (d) Accurate and where necessary kept up to date (Accuracy);
- (e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
- (f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
- (g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation);
- (h) Made available to Data Subjects and Data Subjects are allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

### **4. LAWFULNESS, FAIRNESS, TRANSPARENCY**

#### **4.1. LAWFULNESS AND FAIRNESS**

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

- (a) the Data Subject has given his or her Consent;
- (b) the Processing is necessary for the performance of a contract with the Data Subject;
- (c) to meet our legal compliance obligations;
- (d) to protect the Data Subject's vital interests; or
- (e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

#### **4.2. CONSENT**

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action and so silence, pre-ticked boxes or inactivity will not be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent will need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is generally required for Processing Sensitive Personal Data, for automated Processing and for cross border data transfers. Usually however, we will be relying on another legal basis (and will therefore not require Explicit Consent) to Process most types of Sensitive Data.

#### **4.3. TRANSPARENCY (NOTIFYING DATA SUBJECTS)**

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPM, and how and why we will Process that Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the

GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

## **5. PURPOSE LIMITATION**

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

## **6. DATA MINIMISATION**

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties. Do not collect excessive data and ensure that any Personal Data collected is adequate and relevant for its intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

## **7. ACCURACY**

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or outdated Personal Data.

## **8. STORAGE LIMITATION**

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You must also ensure that Data Subjects are informed of the period for which Personal Data is stored.

## **9. SECURITY, INTEGRITY AND CONFIDENTIALITY**

### **9.1. PROTECTING PERSONAL DATA**

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we hold or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure the security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data, including any such measures that we may prescribe for those purposes. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- (a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;
- (b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed;
- (c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

## **9.2. REPORTING A PERSONAL DATA BREACH**

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches or the DPM. You should preserve all evidence relating to the potential Personal Data Breach.

## **10. TRANSFER LIMITATION**

The GDPR restricts data transfers to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You may only transfer Personal Data outside the EEA if one of the following conditions applies:

- (a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- (b) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- (c) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interests.

## 11. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- (a) withdraw Consent to Processing at any time;
- (b) receive certain information about the Data Controller's Processing activities;
- (c) request access to their Personal Data that we hold;
- (d) prevent our use of their Personal Data for direct marketing purposes;
- (e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- (f) restrict Processing in specific circumstances;
- (g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- (i) object to decisions based solely on automated Processing, including profiling ;
- (j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- (k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- (l) make a complaint to the supervisory authority; and
- (m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the DPM and comply with the Company's Data Subject response process.

## 12. ACCOUNTABILITY



### **12.1. IMPLEMENTATION**

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company has put adequate resources and controls in place to ensure and to document GDPR compliance including:

- (a) appointing an executive accountable for data privacy;
- (b) integrating data protection into internal documents, including this Policy;
- (c) regularly training Company Personnel on the GDPR, this Policy and data protection matters including, for example, Data Subjects' rights, Consent, legal basis and Personal Data Breaches. The Company will maintain a record of training attendance by Company Personnel; and
- (d) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using the results of testing to demonstrate compliance improvement efforts.

### **12.2. RECORD KEEPING**

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's record keeping guidelines.

### **12.3. TRAINING AND AUDIT**

We will ensure Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We will also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

### **12.4. DIRECT MARKETING**

We are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale or prospective sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

## **12.5. SHARING PERSONAL DATA**

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of the Company if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- (a) they have a need to know the information for the purposes of providing the contracted services;
- (b) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- (c) the transfer complies with any applicable cross border transfer restrictions; and
- (d) a contract that contains GDPR approved third party clauses has been utilised.