General Data Protection Regulations Policy

Objective

The purpose and objective of this General Data Protection Regulation Policy is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental, to ensure compliance to the regulations and to minimise the risk of data breaches and any subsequent consequences.

Policy

It is the Policy of Abbey Labels to ensure that:

- Information will be protected from a loss of: confidentiality, integrity and availability, so that it is accessible only to authorised individuals, protected against unauthorised access, the accuracy and completeness and processing methods are safeguarded, and that authorised users have access to relevant information when required.
- Regulatory and legislative requirements will be met.
- Business continuity plans will be produced, maintained and tested.
- Information security training will be available where required.
- All breaches of data security, actual or suspected, will be reported to, and investigated by, the Data Security Manager.
- Guidance and procedures will be produced to support this policy. These may include incident handling, information backup, system access, virus controls, passwords and encryption.
- The role and responsibility of the designated Data Protection Officer (DPO) is to manage data security and to provide advice and guidance on implementation of the General Data Protection Regulation Policy.
- The Data Protection Officer (DPO) is nominated on the current Organisation Plan.
- The designated owner of the General Data Protection Regulation Policy has direct responsibility for maintaining and reviewing it to ensure on-going compliance.
- It is the responsibility of each employee to adhere to the General Data Protection Regulation Policy.

Legal Requirements

Some aspects of data security are governed by legislation, the most notable U.K. Acts are:

- The General Data Protection Regulation (EU) 2016
- Copyright, Designs and Patents Act (1988) as amended
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Human Rights Act (1998)

Scope of the Policy

This Policy applies to all employees, contractors and visitors, to all data held electronically, on paper, transmitted by post, video and verbally, and all types of information and systems.

The Policy applies to all locations from which Abbey Labels systems are accessed (including home use or other remote use).

Where other organisations such as clients or sub-contractors access information held by Abbey Labels, then Abbey Labelsmust either confirm the security policies they operate meet our security requirements or that the risk is understood and mitigated.

Abbey Labels Records

All staff and company records should be stored in a secure area and not left in an unattended. They should only be retained for the minimum length of time that they are absolutely required.

Access control to secure areas

Data held by our Cloud suppliers will be located in a secure environment and shall comply with the same or higher level of security than our own.

Local network equipment / file servers and network equipment will be located in secure areas and where appropriate access controlled.

Unrestricted access to the central computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment. Restricted access may be given to other staff where there is a specific need for such access.

Regular reviews of who can access these secure areas should be undertaken.

Remote Working

Staff contracted to work off site either from home or other locations are to ensure that security arrangements meet our requirements. Work must only be undertaken at home using company laptops, unless otherwise authorised.

Staff should take reasonable care to minimise the risk of theft or damage. During transport equipment should be kept out of sight and not left unattended. Computer equipment or manual data must not be left in a car overnight.

Staff should take all reasonable steps to minimise the visibility of computer equipment from outside the home, and to secure windows and doors when the home is unoccupied.

Computer Equipment

Inactive terminals should be set to time out after a pre-set period of inactivity. Users should log off terminals or PCs when leaving them unattended. PCs or terminals should be secured by a key lock or equivalent control (for example, password access control) when not in use.

Passwords should meet our password policy and be kept strictly private and regularly changed.

Users of portable equipment are responsible for the security of the hardware and the information it holds at all times on or off Abbey Labels premises. Users of this equipment must pay particular attention to the protection of, personnel data and commercially sensitive data.

All important data should be backed up to reduce the impact of loss or theft of portable devices. Devices loaned to employees must be returned when staff leaves.

Equipment, Media and Data Disposal

If a machine has ever been used to process personal data as defined under the General Data Protection Regulations or "in confidence" data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken.

All paperwork should be shredded when no longer required.

Data Backup

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Should information be held on a PC hard drive the PC “owner” is responsible for backups.

Data held in the Cloud is backup by our supplier and held securely.

Archived and recovery data should be accorded the same security as live data. Archived data is information which is no longer in current use, but may be required in the future, for General Data Protection Regulations. Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency.

If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data.

Unauthorised Software.

Abbey Labels will only permit authorised software to be installed on its computers. Computers owned by Abbey Labels are only to be used for work. The copying of leisure software on to computing equipment owned by Abbey Labels is not allowed.

Email / Social Media

Users are responsible for drafting all emails / social media messages carefully, taking into account any form of discrimination, harassment, and defamation of Data Protection issues.

Staff emails / social media messages are a form of corporate communication and therefore should be drafted with the same care as letters. Email is an insecure method of communication with content easily copied, forwarded or archived. Sensitive data should not be sent by this means.

Employees are responsible for virus checking any attachment received before opening. Deletion of old emails must be managed by each individual user, keeping in mind storage levels, archival levels, contractual evidence and legal discovery issues.

Emails should not be sent to large numbers of people unless it is directly relevant to their jobs.

Intent to enforce and monitor

Abbey Labels reserves the right to carry out monitoring exercises on its systems, possibly without prior notice. Monitoring, via email blocking software may be used to block and read any email on Abbey Labels's network at any time. Abbey Labels is committed to ensuring that any monitoring is undertaken with reference to the privacy of the user and with regard to the General Data Protection Regulations, the Regulation of Investigatory Powers Act, the Lawful Business Regulations and the Human Rights Act.

Unauthorised access

We will minimise risks by:

- Installing properly configured firewalls. Firewalls will be configured to protect ports so that only authorised parties can gain access.
- Using virus and content scanners (for e-mails and attachments)
- Checking that protection systems are working properly and by examining their logs
- Systems are updated on a regular basis with patches and hot fixes to ensure the latest known intrusion techniques are countered
- Employing basic housekeeping measures like regular backups, and disabling logon accounts of people as they leave your company
- Making sure staff are trained to spot any unauthorised access
- Reviewing security on a regular basis.

Malware

We will ensure the following are in place:

- Anti-virus software installed on computer systems
- Scanning of all incoming e-mail file attachments
- Regular updates of anti-virus software.
- A facility for checking, quarantining and managing e-mail attached files
- User vigilance and awareness
    - The office will be kept physically secure
    - Staff know who to call if machines become infected.
    - Staff do not attempt to open any suspicious e-mails or attachments; treat as suspicious e-mails from: anonymous senders; strangers addressing you in a familiar manner and non-standard addresses
    - Attachments with .EXE, .SCR, .BAT etc. are normally automatically blocked
    - Staff are wary of any attachments with .EXE, .SCR or VBS file extension names.
    - Spam messages and email abuse should be reported

Signed

Tom Allum

Chairman
Abbey Labels