POTTS PRINT (UK) LTD
DATA SECURITY POLICY

(REVISED EDITION, 2019)

Contents

1 Introduction

1.1 Background

1.2 Data Definition

1.3 The Purpose of This Document

2. Management Responsibility

3. Traceability and Responsibility of Client Data

4. Data Breaches

5. Subject Access Requests

6. Access Control

7. Physical Security

8. Passwords

9. Virus / Malware / Spyware Protection

10. Internet / Network Security

11. System / Server Security

12. Backups

13. Data Retention and Elimination

1. Introduction

1.1 Background

Potts Print (UK) Ltd is a supplier of direct mail, transactional mail, printed business stationery, marketing literature, magazines, catalogues, point of sale and printed packaging. Potts Print (UK) provides digital printing (laser, inkjet and large format), polywrapping and intelligent enclosing capabilities. We have sheet fed lithographic printing presses from one to six colours, full colour digital printing, large format printing and full print finishing facilities including folding, stitching, die-cutting and hand fulfilment.

We also provide storage management, distribution and on-line ordering facilities to our clients.

1.2 Data Definition

For the purposes of this policy, data is defined as any confidential information belonging to Potts or one of its clients. This can be in electronic or hard copy format. This will include personally identifiable information (PII) as specified in the General Data Protection Regulation (GDPR), which came in to force on 25 May, 2018.

1.3 The Purpose of This Document

The purpose of this document is to:

- Establish an approach to data security and management that protects client's data, third party data and Potts Print (UK) data, incorporating the latest requirements as stated in the GDPR;
- Reinforce the culture of data security and the responsibility of Potts as both a data processor and data controller in respect to the GDPR;
- Establish mechanisms and rules that help identify and prevent the compromise of data security and the misuse of data; and
- Help respond to any potential complaints and queries about real or perceived non-compliance with these requirements, including data breaches and subject access requested (SARs).

2. Management Responsibility

2.1 Ian White, Director, is the Potts Print (UK) representative responsible for Data Security.

2.2 Ian White is responsible for security implementation, incident response, risk assessments and periodic user access reviews, and the education of information security policies.

2.3 Carla Armstrong and Ian White are responsible for GDPR compliance and the management of information requested under the GDPR.

2.4 Potts Print (UK) Data Security rules and documentation are reviewed on a 12 monthly basis and are published internally and made available externally upon request.

2.5 All relevant operators are sufficiently trained to ensure they understand data sensitive issues, confidentiality, and the mechanisms to protect client data. This is tailored to the role of the individual within the organisation. There are two levels of training. The first is for Data Processing and IT employees and the second is for General Employees. All employees receive relevant information immediately on joining the organisation, prior to exposure to client data. Records of content, attendance and completion are maintained.

2.6 Violations of the Data Security Policy are recorded and result in disciplinary action as appropriate, in accordance with current defined disciplinary policies, procedures and codes of conduct.

2.7 Members of the Management Team are each responsible for implementing these requirements within their areas of responsibility and for monitoring compliance.

2.8 A signed consent form from each employee allows Potts Print (UK) to store PII on their employees. Only data of a legitimate business interest is stored. Employees have the right to withdraw consent at any time, within the context of the GDPR.

2.9 Data Processing Agreements are issued to all clients who use Potts Print (UK) as a data processor (predominately for Direct Mail purposes). This is signed by both parties confirming each party's responsibilities within the context of the GDPR.

2.10 Data Processing Agreements are issued to all suppliers of Potts Print (UK) who act as a data processor on the company's behalf. This is signed by both parties confirming each party's responsibilities within the context of the GDPR.

3. Traceability and Responsibility Of Client Data

3.1 Potts Print (UK) are committed to their responsibilities as a data processor (for its clients) and as a data controller (for it's staff). Potts uphold stringent security measures. It is advised that all clients password protect any supplied databases, regardless of delivery method. Databases may be presented to Potts on a disk or portable storage device, as an email attachment or uploaded to our Secure File Transfer Protocol site. Potts Print (UK) advise clients to include their unique job number to any databases that are sent to our secure e-mail address (data@potts.co.uk) This e-mail address is only accessible by the IT team and Data Processing employees. If clients send their data directly to their regular Potts contact, it is forwarded to the secure e-mail address and immediately deleted from the original receiving e-mail account.

3.2 All client data is protected upon receipt. The data is transferred to an area of the network which is password protected, so that only the IT Team and Data Processing employees can access it. For direct mail projects, a data health check can be conducted with the use of Address Correction software. Upon request, a copy of the data correction report can be made available.

3.3 All client data is initially handled by the Data Processing Team upon receipt. The handler's name is recorded in the Quality Assurance Check Sheet.

3.4 It is the assigned data handler's responsibility to follow the necessary data security requirements throughout its use in the organisation. These policies are periodically checked by the data security team for compliance with GDPR.

3.5 The client data and its corresponding level of protection are consistent when the data is replicated, processed, moved or renamed. Only the IT Team and Digital Print Department have access to these files.

3.6 Client data is only transferred to a third party with the client's permission. All client data must be encrypted during transfer, transmission or delivery to third parties or to separate systems outside the direct control of Potts Print (UK). Clients may instruct otherwise. In which case, their written instructions must be retained for reference.

3.7 Potts Print (UK) has agreements in place with a local direct mail partners. They are best placed to aid Potts Print (UK) in producing clients' work in the unlikely event of a terminal breakdown. We have these established relationships for business continuity and will always be a last resort. Our partner will contractually uphold our data security policy in the event that their services are required. Permission must be sought from the data controller before this option is taken, in accordance with the GDPR.

3.8 Data will never be transferred outside of the EEA in accordance with the GDPR.

3.9 Violations of the Data Security Policy are fully investigated and employees are formally disciplined if required. Offending employees may be dismissed in-line with Company Policy.

4. Data Breaches

4.1 As a data controller, Potts Print (UK) commit to informing the Information Commissioners Office (ICO) in the event of a data breach, as defined within the GDPR, within 72 hours of becoming aware of the breach.

4.2 Subsequent measures and activity post-breach will be carried out in accordance with the GDPR.

4.3 Should a client require a different notification period for Potts to notify them of a breach affecting their data, this can be agreed in writing via the Data Processing Agreement.

5. Subject Access Requests

5.1 As a data controller, Potts Print (UK) will provide information held on a data subject, if requested, in accordance with the GDPR.

5.2 If a data subject approaches Potts, but is requesting information relating to client's data, Potts will inform the client (data controller) of this SAR and respond accordingly.

6. Access Control

6.1 Any information storage medium has a dedicated owner responsible for its use. Ian White is the dedicated owner of all servers within Potts Print (UK). He is responsible for both the maintenance of the servers and their use. Only employees with Ian White's authorisation have access to the servers, other than designated shared files.

6.2 Access to the Potts Print (UK) network, servers and systems is achieved by individual and unique logins and must require authentication. Authentication is controlled with the use of passwords.

6.3 Users are responsible for the security of their passwords. Users are advised that their passwords must not be written down or recorded in unrestricted media, files or documents.

6.4 Each networked PC, which has access to clients' data, is set to auto logout after a short period of inactivity, in order to protect the data from unauthorised users.

6.5 Network access for visitors to the Potts Print (UK) premises is permitted for internet access only, via guest wifi.

6.6 Access to shared documents on the servers and Tharstern Primo (MIS), by new or temporary employees is restricted, unless absolutely necessary and all employees are required to sign an agreement of awareness of the Data Security Policy on arrival.

6.7 Temporary employees do not have access to areas of the network which contain Client or Potts Print (UK) data.

7. Physical Security

7.1 The building which houses all client data is normally manned 24 hours per day. Reception is locked when unattended. Out of office hours, the internal office doors are locked. The employee entrances are controlled by the use of an electronic key which allows access and monitors which employees are on-shift and on-site. The rear of the building has roller/shutter doors which are securely locked when there are periods of full business shutdown. The fire exits are kept locked at all times, except in times of emergency. A two metre high security fence surrounds the complex. Entrance to the complex is via one gate, which is locked during periods of full business shutdown.

7.2 All visitors must sign upon arrival. Visitors are issued a Visitor Pass/lanyard to help identify them as a visitor. This must be worn at all times during their visit.

7.3 All electronic data is stored on servers which are housed in the Server Room. This room is locked when not manned by IT employees. Only Ian White and IT employees hold a key to this room.

7.4 Potts Print (UK) have an alarm system fitted with contact sensors on all of the access doors and PIR detectors in strategic positions. The alarm alerts the Potts Print (UK) nominated Security Company, who in turn contacts relevant Directors / Managers / Police, if it is triggered.

7.5 CCTV is operational on both sites - see page 31 for the CCTV Policy.

8. Passwords

8.1 Employees and Clients are advised their passwords should be six characters or more in length, using a combination of alpha and numeric characters and containing at least one capital letter.

8.2 Employees must not share their password with any one else, other than their departmental manager and Ian White.

8.3 Employees who have their employment terminated have their accounts terminated as part of a pre-defined exit process.

The employee's computer profile will be searched for important documents and everything else will be deleted, including their accounts. Periodic user access reviews are conducted by the owners of the systems / information.

8.4 All employees to have their own PC login details, along with log in details for all of the systems and programmes that they use.

8.5 All departmental Managers to be aware of teams log-in details. These details to be passed to Ian White, Carla Armstrong and Shaun Johnson. This information is to be compiled via IT, Ian White and Carla Armstrong and will be reviewed annually. A password confirmation slip is included within the introduction and welcome page of this company handbook, so new starters can complete this information once log-in details have been established.

8.6 If an employee changes their password they must notify their departmental Manager so records held can be updated. This is also for security purposes. Failure to provide this information is a disciplinary offence.

8.7 Password review and reset. This will be introduced within particular departments including Digital Media and Digital & Direct Mail Divisions. It will be controlled via IT and Ian White. Passwords will be reset every three months for data security purposes.

9. Virus / Malware / Spyware Protection

9.1 The wilful or incompetent introduction of computer viruses or disruptive/destructive programs into the Potts environment is prohibited. Violators will be formally disciplined in-line with company policy.

9.2 All desktop systems, servers and workstations that connect to the network are individually protected with Sophos Endpoint Protection and Sophos InterceptX. These are approved, licensed anti-virus/anti-malware products which are updated each hour.

9.3 All data, including electronic mail, both incoming and outgoing, is scanned for viruses and harmful code prior to acceptance or release. Emails are scanned by the Sophos applications, which protects the whole network in real time. Our webhosting company additionally checks inbound emails for viruses/spam/malware prior to entering our network.

9.4 Infected data is intercepted and quarantined automatically. Logs of which are delivered to the IT Team.

9.5 Reports are produced on the propagation of viruses and the state of the anti-virus software.

9.6 Normal users are not permitted to interfere with the operation of anti-virus software.

9.7 Automatic virus/malware/spyware scans are used to inspect all servers, workstations and stored data on a daily basis.

10. Internet / Network Security

10.1 All connections to the Internet go through a firewall secured connection point. Potts use a Sophos UTM firewall to ensure the entire network is protected.

10.2 Potts have limited wireless access to the network. This connection is password protected and is made available for guests and Directors/Heads/Managers only. In accordance with this policy the password is changed periodically.

10.3 There is no physical access to switches and routers by unauthorised individuals. They are kept in a secure room, which is controlled by Ian White and the IT team.

10.4 Alteration or additions to the network are only performed by authorised and suitably trained employees.

11. System / Server Security

11.1 All systems connected to the Internet have a licensed vendor supported version of the operating system installed, up to date and concurrent with usage.

11.2 All systems are updated manually on a regular basis to ensure they are current with security patches / updates.

11.3 All software installed is licensed, up to date and concurrent with usage.

11.4 Applications or executable code must not be used or installed without authorisation. Only Ian White or the IT Team are permitted to use executable code.

12. Backups

12.1 A full backup is taken from all servers once a week. Each night an incremental backup is performed. Veritas Backup Exec software is used for this function.

12.2 The backups are saved to an external DAS drive, which is kept securely in one of our other locations. Access to the data on these drives is password protected. Backup data files are stored in an encrypted state (AES-256 bit encryption).

12.3 A log of the backups is automatically generated upon completion detailing whether the backup was successful and also any problems encountered. Backup logs are checked daily.

12.4 Client's data will be stored for no longer than four weeks on this drive. This falls within our data retention policy period.

12.5 All of Potts Print (UK) tiered storage servers are configured as RAID5/6 disc arrays which provides resilience in the event that one of the hard discs containing important data should fail.

12.6 Potts operates a data replication program which covers all business critical servers. Zerto Replication is used for this purpose. The application is configured to have a recovery point objective of 48 hours and a recovery time objective of five minutes. This system protects in real-time against IT failure on the main site. The replication journal history is stored securely at the Company's backup location. Zerto replication files are stored in an encrypted state.

11. Data Retention And Elimination

11.1 The client's original data and any modified files will be completely removed from the network as a result of a monthly cleanse. If data is seen to be 28 days old or older it is deleted. Data can be held for longer periods at the client's request. All requests must be documented and recorded.

11.2 Data retention periods are agreed contractually with clients and suppliers, as required by the GDPR.

11.3 Data which is moved to areas of the business - separate to the main network - and for very specific tasks, is immediately deleted upon completion of the intended task.

11.4 In accordance with the GDPR, data should only be kept for as long as is necessary. Different types of data is held for different retention periods. Some data is required by law to be retained for up to seven years. The latest data retention periods which Potts print (UK) follows is available upon request.

11.5 Emails are archived for 36 months, after which they are securely deleted. Any emails containing PII are forwarded to data@potts.co.uk, as stated in 3.1 of this policy.

11.3 All old computers, drives and media are recycled by a certified company. They ensure that no data can be recovered from the equipment. Certificates of destruction are available on request.

11.4 Printers waste, printouts and material containing client's data is destroyed using a nominated shredding company (Shredit Ltd). Certificates of destruction are available on request.

Name: Ian White

Position: Director; Creative & Digital Media Division; Technical Services Division

Date: 01/05/2019

Name: Carla Armstrong

Position: HR & Corporate Services Director

Date: 01/05/2019

A COPY OF THE LATEST POTTS PRINT (UK) DATA PROTECTION REGISTRATION REPORT IS AVAILABLE UPON REQUEST