Data Protection Policy

Fileder Filter Systems is committed to protecting the rights and privacy of personal data, and to comply with the General Data Protection Regulations (GDPR), Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) and the Payment Card Industry Data Security Standard (PCI DSS).

'Personal data' is any information that can identify an individual, and the legislation effects how we handle information collected from employees, clients, suppliers, temps, contractors and prospective clients. The aim of this policy, and data protection training, is to make employees aware of the key practices for supporting legal compliance.

'Processing' is any operation performed upon personal data, such as collection, recording, organisation, storage, retrieval, dissemination or otherwise making available and the destruction of.

Under the GDPR guidelines, Fileder does not require an official Data Protection Officer, but the Company Secretary will act as the central point of contact for any personal data queries or concerns. Fileder Filter Systems Ltd is a data controller, registered with the Information Commissioner's Office (ICO), who are a governing body for data protection.

Basic principles of data protection: data minimisation, accuracy and security, transparency with data subjects and not keeping data longer than is necessary.

1 Purpose

Fileder demonstrates their accountability for data protection by mapping all personal data held, to validate it has a purpose, assigning one or more of the six lawful bases under GDPR. The information is not used for a different purpose (one the data subject would not expect) and data is managed according to retention periods, so it does not outlive its purpose. Employees are responsible for notifying the Company Secretary of any new categories of personal data collected.

2 Consent

Consent is monitored at Fileder through a SAP BP being made inactive or active and from using marketing selection boxes or, for employees, using Sage People (e.g. consent dropdown to use photos).

3 Housekeeping

To support personal data minimisation and data having a purpose, data is managed according to the retention periods, located in the Appendix, and housekeeping best practices. Employees are encouraged to:

- Set annual Outlook reminders to clear-out personal data in folders that no longer has a purpose
- Send links to documents instead of attaching documents in emails, to avoid copies of personal data in various places
- Only use the Outlook Delete folder for deleted items and use subject folders, or an Archive folder, when in doubt
- Not use the Recycle and Download folders in Explorer as storage folders
- Not record excessive personal details, that add no value, in SAP Activities e.g. instead of saying the person was on jury service, or watching his son's nativity play, state they were unavailable

- As per the Monitoring Equipment Policy (Sage People/Policies & Documents/General Policies), avoid using Company property for personal messages, to avoid a breach in privacy as other people have access to your Inbox
- Use Bcc (blind carbon copy) where email addresses are classified as confidential information, or where you shouldn't disclose who is receiving the content e.g. a direct marketing email, so each recipient cannot see the email address of other recipients
- Not leave personal information on the HR Coordinator's desk

4 Deletion

Data deletion is required by employees to: maintain retention periods, to support the right to be erased, remove consent and to support the Payment Card Industry Data Security Standard.

- Paper copies of financial and HR personal data should be shredded
- Emails with payment details on must be deleted from the Inbox and Deleted Items
- Name (and email address when it contains a name) is to be removed from the SAP BP contact if the account is made inactive, or the person has left, so it is no longer personal data
- Deletions from network folders should also be deleted from the Recycle Bin in Explorer
- Deletions from most NAS shared folders go into Recycle Bin folders and all transactions are logged. Sage Payroll is backed up to a network folder and all network folders are synced to a second NAS box nightly for backup purposes. Two backup NAS Boxes are also synced to Synology Cloud Backup on a nightly basis

5 Subject Access Requests

Requests for copies of the personal data held can be made verbally or in writing, and proof of identity should be provided where applicable. The Subject Access Request procedure *(*Intranet/Resources/Procedures*)* should be followed, with all requests forwarded to the Company Secretary.

6 Privacy Policy

Fileder upholds the GDPR individual's right to be informed through the provision of privacy policies and data protection statements on the Fileder website and employee policies. At the point employees collect personal data, where possible, they should advise the person to view the privacy policy on the Fileder website (or Sage People for employees), which outlines the lawful basis and purpose of personal data being collected, as well as their rights.

7 Reporting Personal Data Breaches

All employees are responsible for reporting personal data breaches, so they can be investigated. Data breaches should be reported to the Company Secretary (via email) who will review as to whether the data subject and ICO should be informed, the latter which, has to be done within 72hrs for major breaches affecting an individual's rights and freedoms. Any breaches are then logged by the Company Secretary in the Data Breach Log and relevant corrective and preventative measures implemented.

The aim of reporting security breaches is for legal compliance, continual improvement review, and to gauge Fileder's data security performance.

Examples of data breaches: leaving telephone order forms with bank details unattended, emailing/posting the wrong person personal data, theft (of an unencrypted device such as a work mobile, or hacking to steal data), data left in an insecure location, disclosure of confidential information, cyber incidents, corruption of data, insecure disposal of paperwork or hardware containing personal data, or an insecure webpage.

8 Data Privacy Impact Assessments (DPIAs)

If Fileder is introducing new processes or technologies that involve personal data, profiling (e.g. lead scoring), automated decision making or special category information (e.g. biometrics and health information), the risks to an individual's data rights and freedom are identified and mitigated where possible through a DPIA. It is a mandatory legal requirement in some cases. A DPIA template is available (Intranet/Resources/Procedures) as well as definitions of the rights and freedoms. The Company Secretary should be notified to assist with the process.
Examples of when a DPIA is required: website collecting contact information, new HR system, customer portal, CCTV monitoring.

9 Sharing Information with Other Companies

If personal data is sent to or shared with other companies, Fileder assess the security of those companies. For companies outside of the EU, Fileder will review their security certifications for a US Privacy Shield or equivalent. Fileder also establishes data protection agreements with third party processors where applicable.

Examples: an Excel sheet of contact details sent to a company for a mail out, using a US company to store data on a US server.

10 Confidentiality

Information will be held securely, with non-disclosure agreements signed by all employees and file access limited according to roles and responsibilities. Disclosure of confidential information is a breach of the disciplinary rules that could result in dismissal. Employees could be criminally liable if they knowingly or recklessly disclose personal information in breach of this policy. Even if accessible, data which is clearly personal (e.g. named folders on the network) should not be viewed unless the job role explicitly requires it e.g. a member of ICT.

11 Bank card and Account Information

Fileder is certified as compliant to the Payment Card Industry Data Security Standard. This is a set of security standards to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. To keep cardholder data secure and confidential, employees must:

- Not telephone record customer bank card details. As Customer Service and Finance calls are recorded, the pause function should be used when taking these details over the phone
- Verify changes in bank account details received via email by phone for all of our outgoing payments
- Delete emails with any bank details/card holder data from both the Inbox and Deleted items
- Only record bank card details in Telephone Order Forms
- Destroy any hard copy Telephone Order Forms containing bank card details by cross-cut shredding
- Not share cardholder data with anyone not directly linked to the credit card payment process or outside the organisation

ICT practices for systems processing credit card information:

- Vendor supplied defaults for system passwords and other security parameters must not be used and must be changed before installing a system on the network
- Vendor supplied defaults for system passwords and other security parameters must not be used and must be changed before installing a system on the network
- Unnecessary default accounts must be removed or disabled before installing a system on the network
- All users should have a unique ID and password
- Access for any terminated users is to be immediately deactivated or removed
- Group, shared, or generic accounts, passwords or other authentication methods are prohibited. Generic user IDs and accounts are disabled or removed. Shared user IDs for system administration activities and other critical functions do not exist. Shared and generic user IDs are not used to administer any system components

12 Security

Wherever personal data is held, whether electronically on the network or in a cupboard, security is considered, including that of the building itself. A documented security risk assessment of Fileder's personal data locations is available for audit purposes and should be added to if new methods of storing personal data are considered. Employees should not introduce new technologies/software/online accounts without going through ICT so they can carry out the necessary risk assessments, which may require a Data Protection Impact Assessment.

Business Continuity and Data Recovery policies provide guidelines on accessing data should disaster recovery be required.

13 Employment References

Company references can be provided up to six years of leaving, with the departing employee's opt-in consent, sought during the exit process (post 2018). References will only detail start/leaving date and positions held.

14 Marketing

Fileder considers the GDPR and PECR when carrying out its marketing activities on cold, new and dormant leads.

- Website forms, and SAP Marketing preference tick boxes, support the monitoring of solicited (requested) marketing which is not affected by PECR.
- Marketing information should not be provided to individuals who have opted out of receiving it (noted in SAP Marketing preferences or telesales activities of inactive SAP BPs)
- For existing customers who have bought from us (or have negotiated in a sale at least), Marketing may use a soft opt-in (without explicit consent). For this, Marketing must use the email address given during sale negotiations, the person is given an opportunity to opt-out of marketing communications in all messages, and the communications relate to similar products/services to what they have purchased
- Telephone leads - should be checked against the Telephone Preference Service (and CTPS), and an opportunity provided to opt-out of future calls. Personal data provided by third parties such as Marketscan is already checked.
- Marketing emails - only sent to the employees of corporates (government, limited or public limited company), under the lawful basis of legitimate interest and include an opt-out from receiving email marketing. For any sole traders, partnerships or residentials who have not previously bought from Fileder, consent is required under PECR regulations.
- Marketing post - is mailed to corporates and only to contacts who have not opted out.

Company Policy

Data Retention Checklist

Data Type	Period of Retention	Disposal Method
Accident books, records and reports	6 years from date of last entry	HR: - Shreds any paper copies - Deletes from HR folder
Biometrics	Delete following employee departure	- ICT delete user and events from Paxton database
CCTV images	CCTV is livestreamed, no records kept	- DAHUA & Nest automatically remove them from their server
Criminal record checks	6 months	- HR shred the paper copies and delete digital records
Drug and alcohol screening results	- negative results 1year - collection process for 2yrs, refusals to test, alcohol tests greater than the acceptable limit and verified positive drug test results 5yrs	HR: - Shreds the paper copies - Deletes emails and records in the HR folder
Email accounts	-Email address 13months after the cessation of employment	ICT: - make the account inactive and archive emails
Facial Temperature Scanner	-Instantly removed for visitors -Instantly removed following cessation of employment	Digital records deleted
Financial information (Includes payslips, reporting, payroll information, childcare, pension and dental plan payments)	7 years	HR / Business Services Assistant: - Shreds any paper copies - Deletes records from Sage Payroll - Annual review SAP invoices/attachments and create a list for IT to delete
Helpdesk tickets	Attachments deleted prior to closing ticket and reviewed annually based on use and relevance to current technology	- ICT electronic deletion
HR employee records and personnel files (Includes training, parental leave, appraisals, disciplinaries, CV, medical information, passport details, driving checks/penalties, dependants and exit interview notes)	- Bank details, photo, personal profile, driving penalties, next of kin and emergency contacts removed after employment ceases - Written warnings 6months, final warnings 1 year or for the length of employment depending upon severity - All other records 6 years after employment ceases	HR: - Shreds any paper copies - Deletes from Sage HR/Sage People - Reviews and deletes from ClassMarker monthly
Intranet	- Reviewed when a person leaves to remove any personal data	HR / Business Services Assistant:

		- Deletes attachments and links from the Media page using the Intranet user log in
Maintenance records	6 years	Business Services Assistant/Facilities Engineer: Delete from system/shred old records containing personal data
Marketscan/lead lists downloaded from suppliers	2 years	Channel Support delete Excel file
Maternity pay records (Mat B1s, certificates, medical evidence)	7 years	HR Manager: - Shreds any paper copies -Deletes records from Sage HR/Sage People
Monitoring records	6 months	Line Manager and HR: - Shred any paper copies and delete electronic
Parental leave	7 years	HR deletes from Sage HR/Sage People
Photographs	- Passport and other individual photos 6 years from cessation of employment - Group and individual work-related photos from company events, minimum 6 years and longer if specific to a purpose cited in exit letter	- HR / Business Services Assistant deletes from Intranet User log in, link and attachment - HR deletes from Sage People - Marketing delete from network drives
Recorded telephone calls	6 months	- RingCentral telephone system automatic scheduled deletion
Records of tests and examinations of control systems and PPE under COSHH	6 years from the test	Deleted from system
Records of work experience for anyone under 18	Kept until they are 21 years	- HR delete from electronic HR files
Risk assessments	6 years or kept permanently, depending upon if risk is no longer present and RA contains personal data (e.g. machinery no longer used, work experience person no longer present)	- Health and Safety representative deletes from Intranet and H:/
SAP BP information for clients and suppliers	6 years after the last active communication, to support any potential civil action claims	- Make the BP Inactive, so it is archived - Clear the name/email addresses containing names from the relevant tabs - Remove any attachments containing personal data
Scanned files	2 days	- Automated script checks every night and automatically deletes everything older than two days

Sickness, absence and near miss records	6 years	- HR delete records from Sage HR/Sage People as part of removing personnel record - Health and Safety representative deletes near miss records from Google sheet
Unsuccessful job applicant information (speculative CVs, job applications, test results, interview notes)	1 year 3 months speculative CVs	HR delete from: - Email - HR folder on the network - Classmarker - Hard copy interview notes/CVs shredded
Visitors log records	30days, as per CCTV records	Each individual department's ID card holder disposes of in office bin
Working time records	2 years from date on which they were made	HR delete from Classmarker
Workplace	As soon as employment has ended	-Account of departed employees is deleted which deletes all of their posts and information -Employees' posts which are critical to business operations are removed as soon as they are no longer required or are superseded

Owner Business Services Department: JE
Date 02-12-2021
Version 3.1