Is the **NEW WAY OF WORKING** putting businesses at more **risk of data breaches?**

Fellowes **Keep it Confidential Survey 2022** . A report on **SHREDDING** in a hybrid working world

Foreward

> “Many organisations that shifted to a remote working model in early 2020 found, there was simply not enough time to carry out suitable risk assessments before making such drastic changes to their working practices”

“Everyone’s focus was on ensuring their services were able to continue rather than considering the risks associated with the necessary changes. Employees also didn’t have time to adjust to the new way of working and several studies have highlighted the bad habits around data security that have been picked up while working from home during the pandemic.

Fast forwarding to 2022 the way we work has evolved quickly, with more of us than ever embracing hybrid working as part of the post-pandemic return to the office. But have companies acted and have processes been adjusted, or is the new way of working putting companies at more risk of data breaches?

The answer to that question is - Yes. Half of our participants in the study believe that hybrid working may have increased the amount of sensitive information being lost or in breach of GDPR rules. Paper documents were not necessarily the first thing companies would worry about when thinking of their security policies, but the swift transition to hybrid working has meant thousands more documents travelling between home and work every week. This raises important questions about confidential paperwork and how we’re protecting it, in a world where a lot of employees no longer work in just the corporate office.

To build on Fellowes’ 40 years of shredder expertise, we wanted to uncover how people are securing and shredding documents in this expanded hybrid working world, as well as how organisations are complying with GDPR (General Data Protection Regulation), 4 years after its implementation. Ever since the early days, we have developed our shredders to meet every workplace need. We are committed to protecting businesses and individuals in any workspace, by helping to prevent paper documents from getting into the wrong hands.

Our research, in partnership with B2B International, covered 605 shredder users across France, Germany and the UK, working in financial services, the public sector and healthcare.

In this report, we will take a deep dive into trends and behaviours around data security in this ever-evolving work environment and we hope we can guide businesses through this phase of change. Because securely destroying sensitive paperwork, wherever you work, is vital to containing the security risks that every organisation faces.”

Steven Hickey

Shredder development timeline

1982
COMMERCIAL SHREDDERS

Fellowes enters licensing agreement with a German company to manufacture commercial shredders

1990
THE FIRST PERSONAL SHREDDER

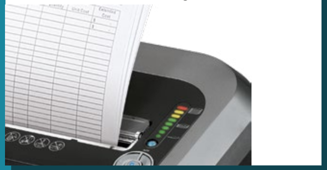
An invention, the personal paper shredder is unveiled

2005
SAFESENSE™

Introduction of Fellowes SafeSense™ Shredder technology makes shredders safer for the home

2008
100% JAM PROOF SHREDDERS

Introduction of Fellowes 100% Jam Proof Shredder Series to eliminate paper shredder jams



2014
AUTOMAX™ AUTOFEED SHREDDERS

Fellowes introduces AutoMax™ AutoFeed Shredders to enhance shredder productivity in the office

2020
LX SERIES

Introduction of Fellowes most advanced micro-cut shredders designed to integrate into any workspace.

GDPR and data protection in a hybrid working world

Our research has shown that **8 out of 10** respondents have adopted remote working, either full or partially. Hybrid working – a combination of on-site and remote working – may have brought more flexibility and variety in choice of workplace, but it also presents the on-going challenge of ensuring people understand confidential working and applying of good data protection principles, in all locations.

Whether your staff are working in the office, at home, in shared working spaces or anywhere else, you need to manage their security risks. This starts with making sure you look at some of the areas that might cause new risk to your organisation. For example, you should have strict policies around staff using their own computers, tablets and smartphones for work purposes as you will have less corporate control over how those devices are configured and used. Another area of concern is the use of public and home Wi-Fi, as well as weak and reused passwords. Both areas are a common point of intrusion for cyber-attacks and clear instructions have to be shared with employees to make sure they and the business are protected.

To no surprise to us, paper documents pose one of the most underrated risks to companies. With everything being digital nowadays people often forget to include the element of paper data in their security policy. However, it is important to highlight that the majority of businesses (68%) that have taken part in our study have indicated that they handle a large amount of sensitive printed information on a daily basis. **70%** of all respondents have either taken printed work documents home, printed work documents at home or both and just shy of half of this group has then put these documents in a

Not sure about the details of GDPR? We have you covered...

The General Data Protection Regulation was introduced in May 2018 and is a comprehensive set of data protection requirements for the handling of European citizens' personal data. Any organisation that handles this personal data must only collect it under strict conditions, for legitimate purposes and protect it from misuse.

Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

What is Personal data?

Personal data is data related to a living individual who can be identified from that data. This could include names, addresses, social security numbers, social media details, CCTV, or photographs. Personal data can be in digital or paper form.

What are the consequences of not complying with GDPR?

A personal data breach can result in fines of **4% of global turnover or €20 million**, as well as a damaged business reputation.

Six principles of data protection

Every data protection strategy should include the principles that data shall be:

- Processed lawfully, fairly and in a transparent way
- Collected for specific, explicit, and legitimate purposes, and not subsequently processed in a way that goes against those purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and up to date. Inaccuracies should be processed, erased, and rectified
- Kept for no longer than is necessary
- Processed securely

Find out more at General Data Protection Regulation - Fellowes®

wastepaper or recycling bin without shredding them. Furthermore, **46%** of all respondents have seen people leave confidential work-related documents unattended. This should be of big concern to businesses. Even if there seems to be strict policies on shredding sensitive information across European companies, these guidelines are often not followed outside of the office. Whether it's in a corporate office or home workspace, sensitive paper data must be locked away when not in use, and securely shredded once it is no longer needed for the purpose it was acquired.

Our study also has revealed, that even after 4 years – only **60%** overall are familiar with GDPR and just **1 in 4** businesses have adapted their policies to include home working or remote working in general. Regulators such as the Information Commissioner's Office (ICO) made allowances for the pressure the pandemic put businesses under. However, with most restrictions being lifted across Europe, the ICO will be less lenient, so it is essential to act now if you are making hybrid working permanent. You need to make sure that polices are reviewed and updated so that it reflects the new way of working and covers potential data breach risks.

Once these policies are updated it is important to have a strong implementation and communication plan in place. The research highlighted a clear disconnect within organisations. Whereas the majority (83%) of respondents in more senior job roles seemed to be aware of GDPR and would actively follow the companies' data protection rules and regulations, only **57%** of respondents in more junior roles where familiar with GDPR and therefore would not be following the guidelines, no matter the working location.

Communication and control of what happens with sensitive documents and data often seems easier when working in the office together with the whole team. But a fact is that hybrid working is here to stay, and business should embrace it to support their workforce. At the same time, it is imperative that processes and regulations are adapted to reflect these changes. The consequences of sensitive paperwork going astray are far-reaching, making it vital for education about this regulation to be cascaded to all colleagues, at every level- because it only takes one piece of misplaced data to lead to a breach. In the next section, we will offer suggestions on how to go about implementing those changes across the business.

GET GDPR
COMPLIANT

What can businesses do to help their staff be compliant with Privacy and data policies?

Update of policies

Think about your Bring your own device (BYOD) policy - if employees use their own devices when working from home.

Highlight public and home Wifi as a threat and what staff needs to do to use them safely.

Review and adapt your policies around printing, storing and disposal of paper documents and add a section around storage and disposal of documents in the home office.

Review your password security policies. The National Cyber Security Centre (NCSC) currently recommends using three-word passphrases rather than passwords. Additionally, you should consider multifactor authentication.

Your policy should state that before disposing of, selling or donating an old computer or hard drive, all data has to be fully erased from the hard disk.

Training

Don't assume everyone understands GDPR. Educate all employees on GDPR requirements, personal data handling and the six principles of data protection. Training should be given to all new starters and as part of regular data security refresher sessions.

Provide a checklist for your employees of areas that could pose a risk for a data breach - you could also let them do a **Data Security Health check**.

Make sure your training covers sensitive paper documents and how to handle these. Which documents and records need to be stored for fixed amounts of time and which ones should be destroyed straight after they are no longer needed.

Add a training module around data security in the home office that highlights the new additions to your policies.

Consider an online training portal so you can track the status of everyone's training and set a fixed deadline.

Equipment

To avoid issues with BYOD we would advise for the company to invest in laptops rather than desktops- this way the equipment can easily be taken in between the home and the corporate office.

Invest in superior anti-virus and firewall systems

Make sure that your staff has access to a shredder in the corporate office. Additionally, employees working from home should be equipped with a small or home office shredder.

For highly confidential or personal data like addresses, invoices and balance sheets opting for a micro-cut (P-5) shredder as the smaller particle size provides superior security making data impossible to read or recover.

Ensure a productive and safe workspace for your employees by taking into account jam prevention and safety features when looking for a shredder.

Communication

Communication is key across all levels of the business. Avoid knowledge gaps in more junior level positions.

Data security should be covered in the next site meeting as well as in smaller groups during the monthly team meetings and 1-1 catch ups.

Put reminder posters up across the business - but also include the update to the policies in your newsletter and post it on your intranet.

Sharing of best practices and any phishing or cyber-attack threats with the business so everyone can watch out for them

Make Data Security part of quarterly business reviews

What can employees do to avoid data breaches?

Understand what Data is sensitive and needs to be protected

Any documents that contain personal data and business records should be safely shredded in line with legal requirements on the retention of data.

Make sure you are aware that every country has its own required period for the storage of contracts, business agreements and similar documents. Once these retention requirements are fulfilled, document destruction is the best way to free up storage space and protect confidentiality.

Receipts, deposit slips and bank statements can usually be shredded once they have been reconciled with accounts.

HR records should be regularly checked, and once they have reached their legal expiry date, they must be destroyed. GDPR requires HR departments to demonstrate why they are keeping data on employees past and present and justify why they are keeping any data beyond the required retention period.

Safe Storage or disposal of paper data

Think before you print. Ask yourself: Do I really need a hard copy of this? Who might accidentally pick up that document?

Shred as you go along, if that is not possible, shred all sensitive paperwork before recycling or disposing of it, ideally without needing to take the risk of transporting it from home to office, or vice versa.

Never leave sensitive paper data lying around unattended at home or in the office. Always clear your desk at night and lock away protectively marked papers and all removable computer media before you leave your workstation.

Regularly review the data you hold and where possible anonymise personal data as soon as it is no longer needed

Keep up to date with training and policies

Make sure you are aware of existing training modules and that you have access to those. Also consider setting set quarterly reminders in your calendar to attend refresher sessions.

Encourage colleagues and team members to attend training, as well as remind each other about the rules and guidelines should you notice someone not acting withing the policy (e.g. leaving sensitive documents lying around, using personal devices etc)

Make yourself familiar with the six principles of data protection

Speak to your manager or data protection officer if you have any questions

Key takeaways from our study

8 out of 10

of all respondents have adopted home working.

70% of all respondents have either taken printed work documents home, printed documents at home, or both.

47%

of those **don't shred work documents** after finishing with them **>>> Leading to security risks during transit!**

46%

have seen people leave **confidential work-related documents unattended**

There is a big **lack of awareness of GDPR in Junior or non-managerial roles**

Only 57%

say they are familiar with the regulation

After 4 years

Only 60%

of all respondents say they are aware of GDPR.

Four in ten (41%)

say they still have not experienced a formal update to the

GDPR policy for home working.

Guidance for better shredding practices:

Secure shredding is key to keeping confidential paperwork out of the wrong hands and reducing organisational exposure to data breaches. In an era when more people than ever are working hybrid-fashion, between home and office, yet complying with GDPR matters as much as ever, the data security risks this presents are clear.

Using a shredder to safely destroy confidential paperwork should be part of our daily routine, wherever we work.

- Don't assume everyone understands GDPR. Educate all employees on GDPR requirements, personal data handling and the six principles of data protection. This training should be given to all new starters, whenever legislation is updated, and as part of regular data security refresher sessions.
- Lock confidential documents away when these are not in use, and never leave them lying around unattended at home or in the office.
- Shred all sensitive paperwork before recycling or disposing of it, ideally without needing to take the risk of transporting it from home to office, or vice versa.
- Give all employees easy access to a secure shredder at home and at work.

Find the right shredder for your work environment.
Vistit www.Fellowes.com or click **here**

Keep it Confidential Survey 2022

Methodology

The research has been conducted by B2B International in April 2022. 605 shredder users have been questioned, with an equal split across the UK, France and Germany. The focus has been on shredder users across different seniority levels of small to mid-size companies from the following sectors - financial services (206) , the public sector(206) and healthcare/medical (193).
To be able to compare working habits around data security in a hybrid working world, it was important to have an equal split across people working between home and the office, working mostly in a corporate office, only in a corporate office, mostly at home or only at home.

For any further details on the methodology split please get in touch with jdettler-bates@fellowes.com

Fellowes®

www.fellowes.com