# Besteht für Unternehmen ein erhöhtes **Datenschutzrisiko durch die neue Arbeitsweise?**

Fellowes

**„Datenschutz einhalten“-Umfrage 2022**. Ein Bericht zum Thema **Aktenvernichtung** in hybriden Arbeitswelten.

# Vorwort

> Viele Unternehmen, die ihre Beschäftigten Anfang 2020 ins Homeoffice geschickt haben, hatten einfach nicht genug Zeit, um vor diesen drastischen Änderungen ihrer Arbeitspraktiken angemessene Risikobeurteilungen durchzuführen.

„Im Mittelpunkt standen Bemühungen, die Arbeit fortzuführen, anstatt Risiken zu erwägen, die mit den erforderlichen Änderungen verbunden waren. Die Beschäftigten hatten ebenfalls keine Zeit, sich auf die neue Arbeitsweise einzustellen. Verschiedene Studien haben auf die schlechten Gewohnheiten hingewiesen, die im Hinblick auf die Datensicherheit während der Pandemie durch die Arbeit im Homeoffice entstanden.

Bis 2022 entwickelte sich unsere Arbeitsweise schnell weiter und mehr Beschäftigte als je zuvor arbeiten auch nach der Pandemie hybrid. Haben Unternehmen nun die entsprechenden Maßnahmen ergriffen, wurden Prozesse angepasst oder besteht für Unternehmen ein erhöhtes Datenschutzrisiko durch die neue Arbeitsweise?

Die Antwort auf diese Frage lautet: Ja. Die Hälfte der Teilnehmenden an unserer Studie glaubt, dass durch hybrides Arbeiten mehr sensible Informationen verloren gehen oder gegen die DSGVO verstoßen wird. Papierunterlagen standen nicht unbedingt an erster Stelle der Sicherheitsüberlegungen von Unternehmen, aber die rasche Umstellung auf hybride Arbeit bedeutete, dass in jeder Woche tausende zusätzliche Dokumente zwischen Homeoffice und Büro unterwegs waren. Das wirft wichtige Fragen über vertrauliche Papierunterlagen und deren Sicherheit auf, in einer Welt, in der viele Mitarbeitende nicht länger ausschließlich im Büro arbeiten.

Wir wollten an 40 Jahre Erfahrungen mit Aktenvernichtern anknüpfen und herausfinden, wie Dokumente in dieser erweiterten hybriden Arbeitswelt gesichert und geschreddert werden und wie Unternehmen die DSGVO (Datenschutz-Grundverordnung) vier Jahre nach deren Inkrafttreten umsetzen. Seit jeher haben wir Aktenvernichter entwickelt, die alle Arbeitsanforderungen erfüllen. Unser Ziel ist es, Unternehmen und Personen in allen Arbeitsbereichen zu schützen, indem wir verhindern, dass Papierunterlagen in die falschen Hände gelangen.

Unsere Studie in Partnerschaft mit B2B International umfasste 605 Nutzer von Aktenvernichtern in Deutschland, Frankreich und Großbritannien, die im Bereich Finanzdienstleistungen im öffentlichen Sektor und im Gesundheitswesen tätig waren.

In diesem Bericht analysieren wir Trends und Verhaltensweisen rund um die Datensicherheit in einer sich ständig entwickelnden Arbeitsumgebung, und wir hoffen, dass wir für Unternehmen in dieser Phase des Wandels wegweisend sein können. Denn die sichere Vernichtung von sensiblen Papierunterlagen ist unabhängig vom Arbeitsort sehr wichtig, um die Sicherheitsrisiken, die alle Unternehmen betreffen, zu minimieren."

**Steven Hickey**

## Aktenvernichter-Entwicklung im Zeitverlauf

### 1982
**GEWERBLICHE AKTENVERNICHTER**

Fellowes schließt einen Lizenzvertrag mit einem deutschen Unternehmen zur Herstellung von gewerblichen Aktenvernichtern ab

### 1990
**DER ERSTE PERSÖNLICHE AKTENVERNICHTER**

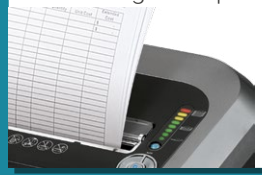
Eine Erfindung, der persönliche Aktenvernichter, wird vorgestellt

### 2005
**SAFESENSE™**

Die Einführung der Fellowes SafeSense™ Aktenvernichter-Technologie macht Aktenvernichter für den Heimgebrauch sicherer


### 2008
**100 % STAUFREI AKTENVERNICHTER**

Einführung der Fellowes 100 Prozent Anti-Stau Aktenvernichter-Serie zur Vermeidung von Papierstaus



### 2014
**AUTOMAX™ AUTOFEED AKTENVERNICHTER**

Fellowes stellt den AutoMax™ Autofeed Aktenvernichter vor, der die Produktivität von Aktenvernichtern im Büro verbessert

### 2020
**LX-SERIE:**

Die Einführung der fortschrittlichsten Fellowes Aktenvernichter mit Mikroschnitt, die sich in jeden Arbeitsbereich integrieren

# DSGVO und Datenschutz in einer hybriden Arbeitswelt

Unsere Untersuchungen haben ergeben, dass **8 von 10** Befragten entweder komplett oder teilweise Telearbeit verrichten. Hybrides Arbeiten – eine Kombination aus Arbeiten im Büro und außerhalb des Büros – hat zu mehr Flexibilität und Abwechslung bei des Wahl des Arbeitsplatzes geführt. Es ist aber auch mit der ständigen Herausforderung verbunden, Beschäftigten die Grundsätze des vertraulichen Arbeitens zu vermitteln und an allen Orten gute Datenschutzpraktiken umzusetzen.

Sie müssen die Sicherheitsrisiken Ihrer Mitarbeitenden verwalten, ob diese nun im Büro, im Homeoffice, in Co-Working-Spaces oder an anderen Orten arbeiten. Das beginnt damit, dass Sie sich mit einigen Themenbereichen beschäftigen, die zu neuen Risiken für Ihr Unternehmen führen könnten. Beispielsweise müssen Sie strenge Regeln für die Verwendung privater Computer, Tablets und Smartphones für Arbeitszwecke haben, da Sie als Unternehmen weniger Kontrolle darüber haben, wie diese Geräte eingerichtet sind und verwendet werden. Ein weiterer Problembereich ist die Nutzung öffentlicher und privater WLAN-Verbindungen sowie schwacher und wiederverwendeter Passwörter. Beide Bereiche sind häufige Angriffspunkte für Cyberattacken. Deshalb müssen die Mitarbeitenden zum eigenen und zum Schutz des Unternehmens klare Anweisungen erhalten.

Wir sind nicht überrascht, dass Papierunterlagen ein oftmals unterschätztes Risiko für Unternehmen darstellen. Da heutzutage alles digital ist, vergessen die meisten, Daten in Papierform in ihre Datenschutzrichtlinie aufzunehmen. Wir möchten allerdings darauf hinweisen, dass die Mehrheit der an der Studie beteiligten Unternehmen (68 %) angaben, dass sie täglich viele ausgedruckte sensible Informationen handhaben. **70%** aller Befragten haben entweder ausgedruckte Arbeitsunterlagen mit nach Hause genommen, Arbeitsunterlagen zu Hause ausgedruckt oder beides.

## Sie kennen die Einzelheiten der DSGVO nicht? Wir helfen Ihnen gern ...

Die Datenschutz-Grundverordnung trat im Mai 2018 in Kraft. Dabei handelt es sich um umfassende Datenschutzvorschriften für den Umgang mit personenbezogenen Daten in der Europäischen Union. Unternehmen, die diese personenbezogenen Daten handhaben, dürfen sie nur unter strengen Bedingungen und zu legitimen Zwecken erheben und müssen sie vor Missbrauch schützen.

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten durch geeignete technische und organisatorische Maßnahmen gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Beschädigung.

### Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die sich auf eine lebende, anhand dieser Daten identifizierbare Person beziehen. Dazu gehören z. B. Namen, Adressen, Sozialversicherungsnummern, Social-Media-Details, Videoüberwachungsaufnahmen oder Fotografien. Personenbezogene Daten existieren in digitaler oder in Papierform.

### Was sind die Folgen der Nichteinhaltung der DSGVO?

Eine Verletzung des Schutzes personenbezogener Daten kann zu Strafen in Höhe von bis zu **4 % des weltweiten Umsatzes oder 20 Millionen Euro** führen und den Ruf des Unternehmens schädigen.

### 6 Grundsätze des Datenschutzes

Jede Datenschutzstrategie muss die Grundsätze enthalten, dass Daten:

- **auf rechtmäßige, ordentliche und nachvollziehbare Weise verarbeitet werden**
- **für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden**
- **dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind**
- **sachlich richtig und auf dem neuesten Stand sind. Ungenauigkeiten müssen unverzüglich bearbeitet, gelöscht oder berichtigt werden**
- **nicht länger als für den Zweck erforderlich gespeichert werden**
- **sicher verarbeitet werden**

*Erfahren Sie mehr unter* ***Datenschutz-Grundverordnung – Fellowes®***

Und knapp die Hälfte dieser Gruppe hat diese Dokumente dann in einen Papierkorb oder einen Recyclingbehälter entsorgt, ohne sie zu schreddern. Außerdem haben **46 %** aller Befragten beobachtet, dass Andere vertrauliche Arbeitsunterlagen unbeaufsichtigt ließen. Das sollte Unternehmen zu Denken geben. Selbst wenn es strenge Vorschriften bezüglich der Vernichtung sensibler Informationen in europäischen Unternehmen gibt, werden diese Vorschriften außerhalb des Büros häufig nicht befolgt. Im Büro und im Homeoffice müssen sensible Daten in Papierform weggeschlossen werden, wenn sie nicht benutzt werden, und sicher geschreddert, wenn sie nicht länger für den ursprünglichen Zweck benötigt werden.

Unsere Studie ergab auch, dass selbst vier Jahre nach Einführung insgesamt nur **60 %** mit der DSGVO vertraut sind und nur **1 von 4** Unternehmen das Homeoffice oder die Telearbeit in ihre Richtlinien aufgenommen haben. Datenschutzbehörden wie das Information Commissioner's Office (ICO) in Großbritannien haben den Druck berücksichtigt, dem Unternehmen während der Pandemie ausgesetzt waren. Da die meisten Einschränkungen aber mittlerweile in ganz Europa aufgehoben wurden, werden die Datenschutzbehörden weniger nachsichtig sein. Deshalb müssen Sie jetzt handeln, wenn Sie hybrides Arbeiten auf Dauer beibehalten wollen. Sie müssen sicherstellen, dass Richtlinien überprüft und aktualisiert werden, sodass sie die neuen Arbeitsweisen widerspiegeln und mögliche Datenschutzrisiken berücksichtigen.

Nach der Aktualisierung dieser Richtlinien ist ein guter Plan für die Umsetzung und die Kommunikation entscheidend. Die Studie wies auf ein klares Missverhältnis innerhalb der Unternehmen hin. Während die Mehrzahl (83 %) der Befragten in höhergestellten Positionen die DSGVO kannte und die Datenschutzregeln und -vorschriften des Unternehmens aktiv befolgte, waren nur **57 %** der Befragten in untergeordneten Positionen mit der DSGVO vertraut und befolgten deswegen die Vorschriften unabhängig vom Arbeitsort nicht.

Die Kommunikation und Kontrolle darüber, was mit sensiblen Unterlagen und Daten passiert, ist oftmals einfacher, wenn man mit dem gesamten Team im Büro zusammenarbeitet. Da das hybride Arbeiten fortbestehen wird, müssen Unternehmen ihre Beschäftigten dabei unterstützen. Gleichzeitig ist es unerlässlich, dass Prozesse und Vorschriften an diese Veränderungen angepasst werden. Die Folgen von verlorengegangenen sensiblen Papieren sind weitreichend, sodass die Kolleginnen und Kollegen auf allen Ebenen über diese Vorschrift aufgeklärt werden müssen, denn schon ein verlegtes Dokument kann zu einer Verletzung des Datenschutzes führen. Im nächsten Abschnitt geben wir Empfehlungen, wie diese Änderungen im Unternehmen umgesetzt werden können.

Handeln Sie
**DSGVO KONFORM**

# Was können Unternehmen tun, damit ihre Mitarbeitenden nicht gegen Datenschutzrichtlinien verstoßen?

## Richtlinien

Denken Sie über Ihre Bring-your-own-device (BYOD) Richtlinie nach, falls Mitarbeitende ihre privaten Geräte im Homeoffice verwenden.

Weisen Sie auf die Gefahren von öffentlichem und privatem WLAN hin und wie Mitarbeitende es sicher nutzen können.

Überprüfen und aktualisieren Sie Ihre Richtlinien zum Ausdrucken, zur Aufbewahrung und Entsorgung von Papierunterlagen und fügen Sie einen Abschnitt zur Aufbewahrung und Entsorgung von Unterlagen im Homeoffice hinzu.

Überprüfen Sie Ihre Richtlinien zur Passwortsicherheit. Die von der Deutschen Gesellschaft für Cybersicherheit (DGC) aktuell empfohlenen Passwortkombinationen beinhalten mindestens zehn Zeichen und kombinieren Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen. Außerdem sollten Sie die Multi-Faktor-Authentifizierung in Betracht ziehen.

Ihre Richtlinie sollte beschreiben, dass vor der Entsorgung, dem Verkauf oder der Spende eines alten Computers oder einer Festplatte alle Daten komplett von der Festplatte gelöscht werden müssen.

## Schulungen

Setzen Sie nicht voraus, dass alle die DSGVO verstehen. Informieren Sie alle Mitarbeitenden über die Anforderungen der DSGVO, den Umgang mit personenbezogenen Daten und die sechs Grundsätze des Datenschutzes. Schulungen sollten für alle Neulinge und im Rahmen der regelmäßigen Auffrischungskurse zum Datenschutz durchgeführt werden.

Geben Sie Ihren Mitarbeitenden eine Checkliste für Bereiche, die ein mögliches Risiko für Datenschutzverletzungen darstellen. Die Mitarbeitenden könnten ebenfalls eine **Sicherheitsüberprüfung** durchführen.

Stellen Sie sicher, dass Ihre Schulungen sensible Unterlagen in Papierform und den Umgang mit ihnen abdecken. Welche Dokumente und Unterlagen für einen festgelegten Zeitraum aufbewahrt und welche sofort vernichtet werden müssen, nachdem sie nicht mehr benötigt werden.

Fügen Sie ein Schulungsmodul zur Datensicherheit im Homeoffice hinzu, das die neuen Ergänzungen Ihrer Richtlinie hervorhebt.

Ziehen Sie ein Online-Schulungsportal in Erwägung, damit Sie den Schulungsstatus aller Mitarbeitenden kennen und eine Frist festlegen können.

## Ausrüstung

Um Probleme mit BYOD zu vermeiden, empfehlen wir, dass Unternehmen in Laptops und nicht in Desktop Computer investieren. Auf diese Weise können die Geräte leicht zwischen Homeoffice und Büro transportiert werden.

Investieren Sie in ausgezeichnete Virenschutz- und Firewall-Systeme.

Stellen Sie sicher, dass Ihre Beschäftigten im Büro Zugang zu einem Aktenvernichter haben. Mitarbeitende, die im Homeoffice arbeiten, sollten darüber hinaus einen kleinen Schredder für das Homeoffice haben.

Entscheiden Sie sich bei streng vertraulichen oder personenbezogenen Daten wie Adressen, Rechnungen und Bilanzen für einen Aktenvernichter mit Mikroschnitt (P-5). Die geringere Partikelgröße gewährleistet höhere Sicherheit, da Daten nicht gelesen oder wiederhergestellt werden können.

Gewährleisten Sie einen produktiven und sicheren Arbeitsplatz für Ihre Mitarbeitenden, indem Sie bei der Auswahl eines Aktenvernichters auf die Vermeidung von Papierstau und andere Sicherheitsfunktionen achten.

## Kommunikation

Kommunikation ist auf allen Unternehmensebenen wichtig. Verhindern Sie Wissenslücken in untergeordneten Positionen.

Die Datensicherheit sollte bei der nächsten Betriebsversammlung sowie in kleineren Gruppen während der monatlichen Teambesprechungen und in Einzelgesprächen behandelt werden.

Hängen Sie im Unternehmen Plakate zur Erinnerung auf. Weisen Sie zudem in Ihrem Newsletter auf die Aktualisierung der Richtlinien hin und veröffentlichen Sie sie im Intranet.

Teilen Sie bewährte Praktiken sowie Hinweise auf Phishing- oder Cyberangriffe mit dem Unternehmen, sodass alle danach Ausschau halten.

Beziehen Sie die Datensicherheit in Ihre vierteljährlichen Geschäftsberichte ein.

# Was können die Mitarbeitenden tun, um Datenschutzverletzungen zu vermeiden?

## Zur Kenntnis nehmen, welche Daten schützenswert sind

Alle Dokumente, die personenbezogene Daten und Geschäftsunterlagen enthalten, sollten im Einklang mit den gesetzlichen Bestimmungen über die Aufbewahrung von Daten sicher vernichtet werden.

Sie müssen wissen, dass jedes Land seine eigenen Aufbewahrungsfristen für Verträge, Geschäftsvereinbarungen und ähnliche Dokumente hat. Nachdem diese Aufbewahrungspflichten erfüllt wurden, ist die Vernichtung der Dokumente die beste Möglichkeit, um mehr Platz zu schaffen und die Geheimhaltung zu gewährleisten.

Quittungen, Einzahlungsbelege und Bankauszüge können normalerweise geschreddert werden, nachdem die Konten abgeglichen wurden.

Personalunterlagen müssen regelmäßig überprüft werden. Wenn sie die gesetzlich vorgeschriebene Ablauffrist erreicht haben, müssen sie vernichtet werden. Die DSGVO verlangt von Personalabteilungen den Nachweis, warum Daten von früheren oder derzeitigen Mitarbeitenden aufbewahrt werden sowie eine Stellungnahme, warum Daten über die vorgeschriebenen Aufbewahrungsfristen hinweg aufbewahrt werden.

## Daten in Papierform sicher aufbewahren oder entsorgen

Denken Sie nach, bevor Sie etwas ausdrucken. Fragen Sie sich: Brauche ich das wirklich in Papierform? Wem könnte das Dokument durch Zufall in die Hände geraten?

Schreddern Sie regelmäßig, was Sie nicht mehr brauchen. Falls das nicht möglich ist, schreddern Sie alle sensiblen Unterlagen in jedem Fall, bevor Sie sie recyceln oder entsorgen, idealerweise ohne sie dazu von zu Hause ins Büro oder umgekehrt zu transportieren.

Lassen Sie sensible Unterlagen im Büro oder zu Hause niemals unbeaufsichtigt herumliegen. Räumen Sie am Ende des Tages immer Ihren Schreibtisch auf und schließen Sie Unterlagen mit Geheimhaltungsvermerken sowie Wechseldatenträger weg, bevor Sie Ihren Arbeitsplatz verlassen.

Überprüfen Sie regelmäßig die in Ihrem Besitz befindlichen Daten und anonymisieren Sie nach Möglichkeit personenbezogene Daten, sobald sie nicht länger benötigt werden.

## Mit Schulungen und Richtlinien auf dem neuesten Stand bleiben

Stellen Sie sicher, dass Sie über aktuelle Schulungsmodule informiert sind und darauf zugreifen können. Richten Sie sich auch vierteljährliche Erinnerungen für die Teilnahme an Auffrischungskursen in Ihrem Kalender ein.

Bitten Sie Kollegen und Teammitglieder, an Schulungen teilzunehmen und erinnern Sie sich gegenseitig an die Regeln und Richtlinien, falls Sie bemerken, dass sich jemand nicht an die Vorschriften hält (z. B. sensible Dokumente liegen lässt, private Geräte verwendet usw.)

Machen Sie sich mit den sechs Grundsätzen des Datenschutzes vertraut.

Wenden Sie sich mit Fragen an Ihren Vorgesetzten oder Datenschutzbeauftragten.

# Wichtigste Erkenntnisse

**8 von 10**
arbeiten von zu Hause aus

**70% der Befragten haben**
gedruckte Arbeitsdokumente nach Hause mitgenommen, zu Hause gedruckt oder beides

**47%**
davon vernichten Arbeitsdokumente nicht, wenn sie nicht mehr benötigt werden > potentielles Sicherheitsrisiko

**46%**
haben beobakchtet, wie Andere vertrauliche Arbeitsdokumente offen liegen gelassen haben

**Es besteht ein großer Wissensmangel über die DSGVO bei jüngeren und nicht-leitenden Angestellten**

**Nur 57%**
sagen, dass sie mit der DSGVO vertraut sind

Nach 4 Jahren

**Nur 60%**
aller Befragten gaben an, dass sie sich der DSGVO bewusst sind

**Vier von zehn (41%)**
sagen, dass sie keine formelle Aktualisierung der

**DSGVO Richtlinien für die Arbeit im Homeoffice erhalten haben**

# Tipps zum Umgang mit vertraulichen Dokumenten:

Sichere Aktenvernichtung ist der Schlüssel zum Schutz vertraulicher Papierdokumente  und zur Vermeidung von Datenschutzverletzungen.

*Der Einsatz eines Aktenvernichters zur Vernichtung vertraulicher Unterlagen sollte zu Ihrer täglichen Routine gehören - unabhängig von Ihrem Arbeitsort.*

- Gehen Sie nicht davon aus, dass jeder die DSGVO versteht. Schulen Sie Mitarbeitende zu Themen wie DSGVO Anforderungen, Umgang mit persönlichen Daten und die sechs Grundsätze des Datenschutzes. Diese Schulung sollte immer dann angeboten werden, wenn ein neuer Mitarbeiter startet, sich die Gesetzgebung ändert oder als Teil von regelmäßigen Datensicherheits-Trainings.
- Schließen Sie vertrauliche Dokumente sicher weg, wenn sie nicht verwendet werden und lassen Sie sie niemals unbeaufsichtigt im Büro oder zu Hause liegen.
- Vernichten Sie alle vertraulichen Unterlagen vor der Entsorgung oder dem Recycling, idealerweise ohne sie dafür zwischen Wohnung und Büro zu transportieren.
- Stellen Sie sicher, dass alle Mitarbeitenden Zugang zu einem Aktenvernichter haben - im Büro und zu Hause.

Finden Sie den passenden Aktenvernichter für Ihre Arbeitsumgebung. Besuchen Sie www.fellowes.com oder klicken Sie **hier**

# Umfrage „Datenschutz einhalten“ 2022
## Methodik

Die Studie wurde von B2B International im April 2022 durchgeführt. Es wurden 605 Nutzer von Aktenvernichtern befragt, die gleichmäßig auf Großbritannien, Frankreich und Deutschland verteilt waren. Im Mittelpunkt standen Nutzer von Aktenvernichtern auf unterschiedlichen Führungsebenen kleiner und mittlerer Unternehmen der folgenden Sektoren: Finanzdienstleistungen (206), öffentlicher Sektor (206) und Gesundheitswesen/Medizin (193).
Um Arbeitsgewohnheiten rund um die Datensicherheit in einer hybriden Arbeitswelt zu vergleichen, war es wichtig, eine ausgewogene Verteilung zwischen folgenden Personengruppen zu haben: arbeiten im Homeoffice und im Büro, arbeiten hauptsächlich im Büro, arbeiten nur im Büro, arbeiten hauptsächlich im Homeoffice, arbeiten nur im Homeoffice.

**Für weitere Einzelheiten zur Aufteilung der Methodik wenden Sie sich bitte an jdettler-bates@fellowes.com**

Fellowes

www.fellowes.com