dampf.consulting
informationssicher.gut.beraten.

# Datenschutz *Compact!* - 02/2021

Das Datenschutzmagazin der dampf. consulting GmbH - Ausgabe 02, April 2021

Liebe Kunden,

um personenbezogene Daten richtig zu schützen, reicht der gute Wille nicht. Man muss genau informiert sein, was man tun darf und was nicht. Wissen Sie zum Beispiel, wie Sie einen Datenträger entsorgen, ohne die darauf befindlichen Daten zu gefährden?

Was Sie beachten sollen, wenn Sie auf die Mails eines ausgeschiedenen Kollegen zugreifen wollen, erfahren Sie in unserem zweiten Beitrag.

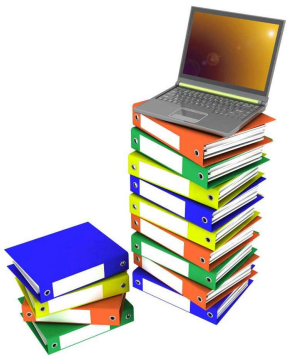
Ebenfalls erfahren Sie in unserer aktuellen Ausgabe, was bei Meldungen von Datenpannen und im Umgang mit Fotos von Beschäftigten zu beachten ist.

Wir wünschen Ihnen viel Spaß beim Lesen!

Ihr Thorsten Dampf, Datenschutzbeauftragter

dampf.consulting
informationssicher.gut.beraten.

# Entsorgung von Datenträgern



**Fehler bei der Entsorgung von Datenträgern gehören unverändert zu den häufigsten Datenpannen. Eine überraschend große Zahl einschlägiger Verletzungsmeldungen an die Aufsichtsbehörden für den Datenschutz zeigt: Die Aufmerksamkeit bei der Entsorgung von Datenträgern darf nicht nachlassen!**

## Papier als klassischer Datenträger

Klassischer „Datenträger" ist Papier. Büros ganz ohne personenbezogene Daten auf Papier sind nach wie vor selten. Fast jeder druckt gelegentlich eine E-Mail aus. Und Notizzettel aller Art finden sich auch fast überall.

All dies landet im Papierkorb. Hoffentlich im richtigen. Denn sollte zum Beispiel für Kunststoffabfälle auch noch ein „gelber Sack" bereitstehen, findet immer wieder so mancher Zettel seinen Weg unzulässigerweise dorthin.

## Altbestände

Oft gibt es noch „Altbestände" in Form von Ordnern voller Papier oder auch in Form von Schachteln voller loser Blätter. Der Grund: Relativ viele Unterlagen müssen aus rechtlichen Gründen eine bestimmte Zeit aufbewahrt werden. Sie sind daher noch vorhanden, obwohl im Übrigen vielleicht inzwischen rein elektronisch gearbeitet wird. Oft genug erfolgt dabei die Aufbewahrung länger, als es rechtlich erforderlich wäre.

## Die Punkt-Methode

Ob Ordner wirklich noch gebraucht werden, lässt sich leicht feststellen. Man legt neben das Ordnerregal Klebepunkte. Wer tatsächlich auf einen Ordner zugreift, bringt auf ihm einen Klebepunkt an. Schon nach einigen Wochen zeigt sich erfahrungsgemäß: Auf fast keinem Ordner klebt ein Punkt.

## CDs und USB-Sticks

CDs und USB-Sticks sind weiterhin in vielen Büros anzutreffen. Das gilt sogar dann, wenn ihre Verwendung längst untersagt wurde und sie die Mitarbeiter mangels entsprechender Anschlussmöglichkeit am PC überhaupt nicht mehr benutzen können.

## Pannen aus schlechtem Gewissen

Solche Datenträger, die eigentlich nicht mehr da sein dürften, werden besonders häufig vorschriftswidrig entsorgt. Irgendwann tauchen sie in Schubladen oder Schränken auf. Man erinnert

sich, dass es einmal eine Anordnung gab, all diese Dinge bis zu einem bestimmten Termin zu entsorgen. Leider geschah das nicht. Und jetzt scheut man sich, das zuzugeben.

Statt die zuständigen Stellen im Unternehmen einzuschalten, geschieht die Entsorgung irgendwie. Schlimmstenfalls im heimischen Hausmüll oder gar im Abfalleimer des nächsten öffentlichen Parks. All dies kommt in der Realität leider vor.

## Entsorgung = Vernichtung

Wesentlich ist bei jeder Entsorgung von Datenträgern, die einschlägigen Vorgaben einzuhalten. Entsorgung bedeutet im Normalfall, dass der Datenträger vernichtet werden muss.

Das geschieht meist durch Zerkleinerung des Datenträgers. Die entsprechenden Vorgaben sind etwas für Fachleute. Der einzelne Mitarbeiter muss sie nicht beherrschen. Es liegt jedoch in seiner Verantwortung, Datenträger an die Stellen im Unternehmen weiterzuleiten, die sich um die Entsorgung kümmern.

## Folgen etwaiger Pannen

Kommt es bei der Entsorgung von Datenträgern zu ernsthaften Pannen, findet das oft große Beachtung in der Öffentlichkeit. Das gilt vor allem dann, wenn Unbefugte beispielsweise Papier aus offenen Behältern mitnehmen konnten. Der Weg des Vorfalls in die Medien ist dann kurz. Zwingende Folge ist zudem eine Meldung an die zuständige Datenschutz-Aufsichtsbehörde, dass der Datenschutz verletzt wurde. All dies lässt sich durch entsprechende Sorgfalt vermeiden.

## Einige unbequeme Fragen

Jede Mitarbeiterin und jeder Mitarbeiter sollte sich mit folgenden Fragen auseinandersetzen:

- Mit welchen Datenträgern, auf denen sich personenbezogene Daten befinden, arbeite ich?
- Welche Datenträger dieser Art bewahre ich auf, obwohl ich sie gar nicht mehr benutze?
- Verfüge ich noch über Daten, deren Vernichtung früher schon einmal angeordnet wurde?
- Kenne ich die Vorgaben dafür, wie lange solche Datenträger aufbewahrt werden müssen?
- Weiß ich, wohin ich Datenträger zur Vernichtung bringen kann?
- Gibt es in unserem Unternehmen irgendwelche Anweisungen oder Vorgaben zu dem Thema (beispielsweise im Intranet)?

## Durchaus darüber reden

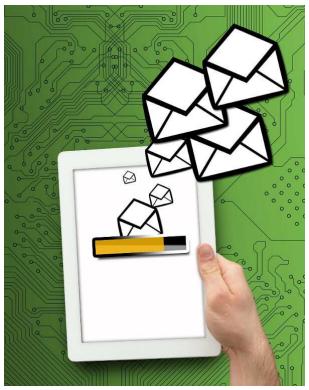
Sinnvoll ist es, das Thema auch mit Kolleginnen und Kollegen einmal zu diskutieren. Dabei stellt sich meist schnell heraus, wo die Schwachstellen liegen, ob am eigenen Arbeitsplatz oder am Arbeitsplatz der Kolleginnen und Kollegen.

### In jedem Fall aber handeln

Wichtig ist es aber, nicht nur zu reden, sondern auch praktische Konsequenzen zu ziehen. Sie können das Thema nicht sofort angehen, weil zu viel anderes zu tun ist? Dann machen Sie sich eine Notiz im Terminkalender, wann Sie auf das Thema zurückkommen wollen. Dann muss es aber wirklich sein!

---

## Zugriff auf E-Mails ausgeschiedener Mitarbeiter



**Der Mail-Account ist noch da, der Mitarbeiter ist aber ausgeschieden. Darf der Arbeitgeber „einfach so" auf die Mails in dem Account zugreifen? Oder ist das nur zulässig, wenn der Mitarbeiter einwilligt? Mit etwas gesundem Menschenverstand lassen sich diese Fragen leichter lösen, als viele befürchten.**

### Im Normalfall: keine Probleme

Normalerweise sollte es so laufen: Ein Mitarbeiter scheidet aus dem Unternehmen aus. Der Grund dafür spielt dabei keine Rolle. In jedem Fall sollte er alle wichtigen Mails einem Kollegen übergeben, der sich künftig um darum kümmert.

### Unerwartete Hindernisse

Manchmal läuft es freilich anders. Dazu ein Beispiel: Die Übergabe der Mails war für den vorletzten Arbeitstag des Mitarbeiters vorgesehen. Leider war der Kollege, der die Mails entgegennehmen sollte, ab dem Tag aber krank. Nun ist der ausgeschiedene Mitarbeiter weg. Den Zugriff auf den Account bekäme die EDV-Abteilung technisch hin. Aber dann tauchen plötzlich Bedenken auf, ob ein solcher Zugriff erlaubt ist.

### Betriebsvereinbarung als Lösung

Falls ein Unternehmen einen Betriebsrat hat, gibt es häufig eine Betriebsvereinbarung zu dem Thema. Aber was, wenn es entweder keinen Betriebsrat gibt oder ausgerechnet dazu keine Betriebsvereinbarung?

### Gegenseitige Rücksicht als Maßstab

Die Antwort fällt relativ leicht, wenn man sich zwei Dinge vor Augen hält:

- In keinem Fall ist der dienstliche Mail-Account eines Mitarbeiters seine reine Privatsache. Der Hauptzweck des Accounts besteht darin, damit Aufgaben für das Unternehmen zu erledigen. Beispiele: Es gehen Bestellungen von Kunden ein oder der Mitarbeiter beantwortet Anfragen von Kunden.
- Andererseits muss ein Arbeitgeber Rücksicht auf die persönlichen Interessen des Mitarbeiters nehmen. Das wird dann wichtig, wenn Mails im Account offensichtlich einen privaten Inhalt haben.

Das Gewicht dieser beiden Aspekte hängt davon ab, ob private E-Mails erlaubt sind oder nicht.

### Verbot privater Mails durch den Arbeitgeber

Am einfachsten ist es, wenn private E-Mails ausdrücklich verboten sind. Dann gehört der Mail-Account gewissermaßen ganz dem Arbeitgeber. Deshalb kann er nach Belieben darauf zugreifen. Eine Einwilligung des ausgeschiedenen Mitarbeiters ist dafür nicht notwendig.

Doch Vorsicht: Auch in solchen Fällen gibt es Grenzen. Klassisches Beispiel: Schon aus dem Betreff einer Mail lässt sich erkennen, dass sie einen rein privaten Inhalt hat. Die Fairness gebietet es, den ausgeschiedenen Mitarbeiter auf die Mail hinzuweisen und sie ihm zu übermitteln, wenn er das möchte.

### Keine „Belohnung eines Regelverstoßes“

Das wirkt auf den ersten Blick etwas merkwürdig. Denn schließlich hat das Unternehmen private Mails doch ausdrücklich verboten. Warum soll es dann Rücksicht nehmen müssen? Nun, kaum jemand kann es völlig verhindern, dass ihm andere Personen private Mails ins Büro schicken. Damit muss ein Arbeitgeber dann in fairer Weise umgehen.

### Erlaubnis privater Mails durch den Arbeitgeber

Komplizierter wird es, wenn der Arbeitgeber private Mails ausdrücklich erlaubt hat. Damit hat er bildlich gesprochen seine Herrschaft über den Mail-Account des Mitarbeiters aufgegeben. Der Arbeitgeber muss in solchen Fällen davon ausgehen, dass ein relevanter Teil der Mails im Account rein privater Natur ist.

### Aufforderung zum „Sortieren“

Die Rücksicht auf die persönlichen Interessen des Mitarbeiters muss deshalb hier im Vordergrund stehen. Vom Grundsatz her darf der Arbeitgeber deshalb nicht auf den Mail-Account des Mitarbeiters zugreifen. Er muss vielmehr mit ihm Kontakt aufnehmen und ihn dazu auffordern, die dienstlichen Mails auszusortieren.

### Berechtigtes Interesse des Arbeitgebers

Daran hat der Arbeitgeber ein berechtigtes Interesse. Denn diese Mails sind notwendig, um die Aufgaben des Unternehmens zu erfüllen. Deshalb darf der ehemalige Mitarbeiter sich auch nicht „einfach so" weigern, seinen früheren Arbeitgeber beim Aussortieren zu unterstützen.

Sollte sich der ehemalige Mitarbeiter dennoch querlegen, kann sein ehemaliger Arbeitgeber durchaus rechtliche Schritte beim Arbeitsgericht einleiten. In dringenden Fällen wäre sogar eine einstweilige Verfügung denkbar.

### Zwei Lösungsmöglichkeiten

Das sind jedoch Extremsituationen, die in der Praxis kaum vorkommen. Im Normalfall einigen sich der ehemalige Mitarbeiter und sein ehemaliger Arbeitgeber einvernehmlich auf eine von zwei Möglichkeiten:

- Entweder erklärt sich der frühere Mitarbeiter mit dem Zugriff einverstanden. Dann sorgt sein Ex-Arbeitgeber dafür, dass lediglich die dienstlichen Mails anhand des Betreffs aussortiert werden.
- Oder der frühere Mitarbeiter greift nochmals auf den Account zu und übernimmt diese Sortierarbeit selbst.

In beiden Fällen sind die berechtigten Interessen beider Seiten gewahrt.

---

## Meldung von Datenpannen

**Die DSGVO hat die Meldepflicht für Datenpannen wesentlich verschärft. Was geht das den „normalen Mitarbeiter" an? Deutlich mehr, als viele glauben!**

### Versendungspannen sind Klassiker

Versendungspannen gehören zu den häufigsten Datenpannen. Einer der Klassiker: Eine E-Mail soll an eine größere Zahl von Adressaten gehen. Sie sollen nichts voneinander wissen. Doch statt im bcc-Feld landet die Adressatenliste versehentlich im cc- Feld. Die Folge: Jeder Adressat sieht die Mailadressen aller anderen Adressaten!

### Eher selten nötig: Benachrichtigung der betroffenen Personen

Rückgängig machen lässt sich das nicht mehr. Also rasch eine Entschuldigungsmail an alle Adressaten und alles ist gut? So einfach ist es nicht! Rechtlich gesehen stellt eine solche E-Mail eine Benachrichtigung der betroffenen Personen dar. Eine solche Benachrichtigung wäre jedoch oft gar nicht nötig. Vorgeschrieben ist sie laut Datenschutz-Grundverordnung (DSGVO) nur, wenn die Datenpanne für die betroffenen Personen voraussichtlich ein „hohes Risiko" zur Folge hat (Art. 34 Abs. 1 DSGVO). Doch das ist eher selten der Fall.

Angenommen, es geht um eine Liste von Personen, die regelmäßig Sonderangebote per Mail erhalten. Dann liegt im Normalfall kein hohes Risiko vor. Denn was soll hier schon passieren? In solchen Fällen ist eine Benachrichtigung eine Frage der Höflichkeit, nicht eine Frage des Rechts.

### Stets eilig: Meldung an die Datenschutzaufsicht

Viel wichtiger ist eine Meldung der Datenpanne an die Datenschutzaufsicht. Für sie gilt:

- Grundsätzlich ist eine solche Meldung bei jeder Datenpanne erforderlich.
- Eine Ausnahme greift nur dann, wenn die Panne voraussichtlich zu keinerlei Risiko für die betroffenen Personen führt.

### Die tückische 72-Stunden-Frist

Hinzu kommt noch folgende Tücke: Für die Benachrichtigung der betroffenen Personen ist keine Frist vorgeschrieben, für die Meldung der Datenpanne an die Datenschutzaufsicht dagegen schon! Sie muss im Normalfall binnen 72 Stunden erfolgen (Art. 33 Abs. 1 DSGVO).

### Keine Meldung durch einzelne Mitarbeiter!

Die Meldung an die Aufsichtsbehörde erfolgt dabei nicht durch den Mitarbeiter, der die Panne verursacht hat! Sie ist vielmehr vom Unternehmen zu veranlassen. Wer innerhalb des Unternehmens zuständig ist, legt die Unternehmensleitung fest.

### Verschweigen? Lieber nicht!

Das scheint auf den ersten Blick Möglichkeiten der Manipulation zu bieten. Sollte man vielleicht möglichst lange Stillschweigen über eine Datenpanne bewahren? Sorgt das dann dafür, dass die 72-Stunden-Frist nicht zu laufen beginnt? Solche Überlegungen sind gefährlicher Unfug. Angenommen, die Unternehmensleitung erfährt erst nach Wochen von einer Datenpanne, meldet sie dann aber sofort an die Aufsichtsbehörde. Hier ist zwar die Meldepflicht formal gesehen erfüllt. Die Aufsichtsbehörde wird dem Unternehmen aber vorwerfen, dass die interne „Pannenorganisation" mangelhaft ist. Denn sonst hätte die Unternehmensleitung sofort von der Panne erfahren.

### Regeln für Mitarbeiter

Die Regeln für jeden einzelnen Mitarbeiter lauten daher:

1. Kehren Sie Datenpannen nie unter den Tisch!
2. Informieren Sie vielmehr sofort die Vorgesetzten!
3. Ist kein Vorgesetzter greifbar, kann der Datenschutzbeauftragte weiterhelfen.
4. Verschweigen macht alles nur schlimmer!

### Wichtige Unterschiede

Wichtig ist, dass die Meldung an die Datenschutzaufsicht und die Benachrichtigung der betroffenen Personen zunächst einmal nichts miteinander zu tun haben. Die Meldung an die Datenschutzaufsicht muss immer rasch erfolgen. Dabei gilt der Grundsatz: Lieber eine Meldung zu viel als eine Meldung zu wenig! Mit der Benachrichtigung der betroffenen Personen sieht es anders aus. Sie verlangt sorgfältige Überlegung und ist bewusst nicht an bestimmte gesetzliche Fristen gebunden.

Meldungen an die Aufsichtsbehörde sind in der Praxis sehr häufig, Benachrichtigungen betroffener Personen dagegen recht selten. Dieser Unterschied beruht zunächst einmal auf den unterschiedlichen gesetzlichen Regelungen. Er lässt sich aber auch aus der Sache leicht erklären:

- Bei der Datenschutzaufsicht arbeiten Profis. Sie können die Dinge einordnen. Wenn eine erste Meldung später teilweise korrigiert werden muss, löst das bei ihnen keine Unsicherheit aus.
- Anders dagegen die Situation der betroffenen Personen. Jede Benachrichtigung verunsichert sie. Sie fragen nach. Kommen dann nur unvollständige Informationen oder Informationen, die später korrigiert werden müssen, hilft ihnen das nicht weiter. Also muss hier gleich alles stimmen.

---

## Fotos von Beschäftigten

**„Fotos von Beschäftigten? Wenn ein Unternehmer die verwenden will, ist immer eine Einwilligung nötig!“ So hört man es häufig. Wenn es nur so einfach wäre! Lesen Sie, in welchen Situationen tatsächlich eine Einwilligung des Beschäftigten nötig ist, in welchen dagegen nicht.**

### Bilder sind personenbezogen

Das Bild einer Person enthält personenbezogene Daten, das ist klar. „Näher dran an der Person“ geht kaum, selbst wenn es sich nur um ein Passbild handelt. Wer das Bild einer Person verwenden will, muss deshalb die Regeln des

Datenschutzes beachten. Dabei besteht unter Juristen über die Ergebnisse eine fast schon erstaunliche Einigkeit – auch wenn sie sich manchmal auf unterschiedliche Paragrafen stützen. Diese Paragrafen kann man deshalb den Juristen überlassen und sich auf das Ergebnis konzentrieren.

### Das Bild im Mitarbeiterausweis

Kann es sein, dass die Verwendung eines Bildes für die Durchführung des Arbeitsverhältnisses erforderlich ist? Wenn ja, kommt es auf eine Einwilligung des Beschäftigten nicht an. Im Gegenteil: Er ist dann aufgrund des Arbeitsverhältnisses verpflichtet, entweder selbst ein Bild zur Verfügung zu stellen oder zumindest dabei mitzuwirken, ein solches Bild anzufertigen.

Typischer Praxisfall: das Bild für den Werksausweis. Ein Werksausweis ohne Bild kann seine Funktion normalerweise nicht erfüllen. Wenn es Mitarbeiterausweis gibt, muss sich der Beschäftigte deshalb dafür fotografieren lassen.

### Das Bild im Telefonverzeichnis

Damit ist aber zugleich der Zweck beschrieben, dem das Bild ausschließlich dienen darf. Nur weil das Unternehmen es „ohnehin schon einmal hat“, darf das Bild nicht einfach für andere Zwecke genutzt werden. Typischer Praxisfall dafür: Es ist zwar schön, wenn man im Telefonverzeichnis des Unternehmens neben dem Namen ein Bild vorfindet. Wirklich nötig ist das aber nicht. Ein Telefonverzeichnis funktioniert auch ohne Bild.

Deshalb setzt ein Bild im Telefonverzeichnis voraus, dass der Beschäftigte damit einverstanden ist. Das darf ein Unternehmen nicht dadurch umgehen, dass es das Bild für den Mitarbeiterausweis „einfach so“ auch für das Telefonverzeichnis nutzt. Dazu muss es den Beschäftigten vorher fragen.

### Das Bild auf der Internetseite

Man ahnt es: Das trifft erst recht zu, wenn Bilder von Beschäftigten auf die Internetseite des Unternehmens sollen. Auch hier gilt: Natürlich ist es schön, wenn man dort beim jeweiligen Amt neben jedem Namen und der zugehörigen Telefonnummer auch ein Bild vorfindet. Erforderlich ist das aber nicht.

Und wie sieht es aus, wenn Beschäftigte an einem Imagefilm des Unternehmens mitwirken sollen? Dazu wird ein Unternehmen schon deshalb niemanden zwingen, weil der „Schauspieler wider Willen“ sonst sicher keine positive Ausstrahlung hat. Unabhängig davon gilt: Ohne Einwilligung geht hier nichts.

### Der Nachweis der Einwilligung

Beim Nachweis einer Einwilligung hat sich übrigens kürzlich ein wichtiger Punkt geändert. Bisher musste eine solche Einwilligung zwingend schriftlich erfolgen. Künftig reicht auch die „elektronische Form“, also etwa eine E-Mail. Schließlich geht das Papierzeitalter allmählich zu Ende.

dampf.consulting
informationssicher.gut.beraten.

**Wenn Ihnen unser Magazin gefallen hat, sagen Sie es gerne weiter**

Unser nächstes Datenschutzmagazin erscheint im Juni!