

Bibliothek
für Designer



DATENSCHUTZ FÜR DESIGNER

Datenschutz verstehen und sicher gestalten

Wie kann ich mein geistiges Eigentum schützen? Was muss ich beachten, wenn ich Inhalte in den sozialen Medien hochlade? Oder herunterlade? Und wie ist das mit dem neuen Datenschutz der DSGVO? Wem überlasse ich meine Daten und wozu? Wie gehe ich mit den Daten meiner geschäftlichen Kontakte um? „Datenschutz für Designer“ gibt dazu Antworten. Hier ein Auszug:

Die gute Nachricht ist: Mit einer Grundausstattung an Formularen und Verhaltensweisen kann auch der Designer relativ einfach einen professionellen Schutz der Daten in seinem Unternehmen gewährleisten.

In technischer Hinsicht gilt – unabhängig von der Größe des Unternehmens – ein erster Grundsatz, wonach der Unternehmer jederzeit wissen muss oder zumindest verlässlich nachvollziehen können muss, wo und wie die von ihm verantworteten personenbezogenen Daten gespeichert und verarbeitet werden.

Beispiele:

- Ein Designer, der als Freelancer arbeitet, konzentriert sich gedanklich zunächst auf seinen Laptop-PC. Tatsächlich speichert und verarbeitet er aber

personenbezogene Daten (bewusst und unbewusst) auch auf verschiedenen USB-Sticks und mobilen Festplatten, auf seinem Tablet, auf seinem Smartphone und sogar auf dem Navigationsgerät seines Fahrzeugs.

- Eine größere Agentur nutzt die Vorteile von Datenverarbeitungsvorgängen in der Cloud mit der Folge, dass ihre personenbezogenen Daten weltweit an verschiedenen Orten gespeichert werden.

Die nötige Bestandsaufnahme dieser Speicher- und Verarbeitungsorte kann mit der Anfertigung des Verzeichnisses erfolgen. Dieses Verzeichnis sollte regelmäßig aktualisiert werden, vor allem nach dem Einsatz neuer Technologien oder Clouddienste. Zudem ist eine gewisse Sparsamkeit und Professionalität im Umgang mit Speichermedien nötig, z.B. die Aufbewahrung aller mobilen

Speichermedien an einem abgeschlossenen Ort, kein „Verleih“ oder gemeinsame Nutzung nur halb gefüllter USB-Sticks, „weil gerade nichts anderes zur Hand ist“, keine Speicherung personenbezogener Daten in fremde Medien wie bspw. in das Navigationsgerät eines geliehenen Fahrzeugs etc.

Ein gut geführtes Verarbeitungsverzeichnis zwingt zur Selbstkontrolle und zur Überprüfung der technischen Verarbeitungsvorgänge.

Der zweite technische Grundsatz zielt auf maximal mögliche Sicherheit der personenbezogenen Daten während des Verarbeitungsprozesses. Natürlich hat der Designer keinen Einfluss auf die inneren Verarbeitungsroutinen der von ihm genutzten Dienstprogramme und die geräteeigene Firmware. Aber Verschlüsselungsmöglichkeiten und sonstige Schutzmaßnahmen sollten in jedem Falle eingesetzt werden.

Beispiele:

- Versand von E-Mails über verschlüsselnde Dienstprogramme;
- Verschlüsselung von E-Mail-Anhängen, sofern diese personenbezogene Daten enthalten;
- Bearbeitungen von Entwürfen nur mit Platzhaltern für personenbezogene Daten und Einsatz der tatsächlichen Daten erst in der finalen Version;
- Vorzug von Kommunikationsmedien, die aktuelle Verschlüsselungsmethoden zur Verfügung stellen (End-to-End-Verschlüsselung, SSL-Standards, Zertifikate etc.);
- Vergabe komplizierter und zufällig generierter Passwörter und Verschlüsselung von Passwortspeichern;
- Einsatz von aktuellen und leistungsfähigen Schutzprogrammen wie Firewall-Technologie, Anti-Spy- und Anti-Phishing-Programme, Trojanerabwehr etc.

Zweiter technischer Grundsatz: Der Designer muss die ihm maximal mögliche technische Sicherheit des Verarbeitungsprozesses gewährleisten.

Sobald dies finanziell möglich ist, sollte sich der Unternehmer durch einen professionellen IT-Dienstleister, der ausreichend zertifiziert ist, technisch beraten lassen. Das betrifft natürlich vor allem die eingesetzte Hardware, aber auch die schützenden Dienstprogramme. Wenn möglich, sollte ausschließlich mit eigenen Servern oder einer rein deutschen Cloudlösung gearbeitet werden. Für Wartungsarbeiten u.ä. ist der IT-Dienstleister Datenverarbeiter und sollte entsprechend zertifiziert sein.

Leider ist es immer noch die Regel, dass „kostenlos“ angebotene Programme meist geringere Sicherheitsstandards aufweisen und – schlimmer noch – gerade mit der Nutzung personenbezogener Daten „bezahlt“ werden. Was für den Designer hinsichtlich seiner eigenen personenbezogenen Daten akzeptabel sein mag, das gilt aber keineswegs für die Daten Dritter, für die er die Verantwortung trägt.

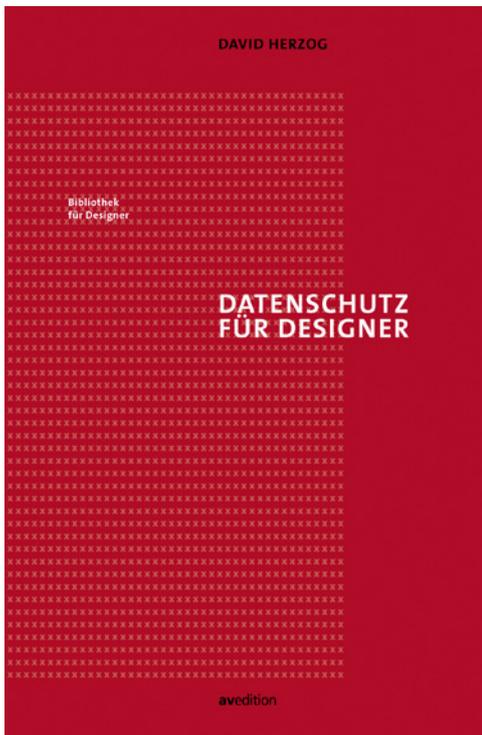
Kostenlose Programme, die tatsächlich mit personenbezogenen Daten Dritter „bezahlt“ werden, dürfen vom Designer nicht eingesetzt werden.

Beispiel:

Beim Kauf eines neuen Smartphone-Modells aus den USA bietet der Store-Mitarbeiter an, die Daten des alten Gerätes komfortabel über die Hersteller-Cloud auf das neue Gerät zu übertragen.

Wenn nun personenbezogene Daten aus dem auch beruflich genutzten Kontaktverzeichnis des alten Gerätes mitübertragen werden, ist dies in der Regel unzulässig gemäß Art. 44 ff. DSGVO. Auch wenn diese Daten nur für kurze Zeit in der USA-Cloud „geparkt“ werden, wird das Gesetz verletzt. Denn die Daten können in dieser Zeitspanne nach US-amerikanischen Gesetzen, die nicht dem DSGVO-Standard genügen, ausgewertet und ggf. unbekannt verarbeitet werden. Im Übrigen müssten auch alle Betroffenen von dieser Zwischenspeicherung in einer außereuropäischen Cloud informiert werden.

David Herzog



Datenschutz für Designer

David Herzog

Deutsch
192 Seiten
Broschiert
14 × 21 cm
ISBN 978-3-89986-355-0

Dieses Buch richtet sich an Gestalterinnen und Gestalter, Kommunikationsdesigner:innen und überhaupt an alle, die mit urheberrechtlich geschützten Werken und/oder personenbezogenen Daten am digitalen Leben teilnehmen wollen. Es vermittelt Kenntnisse, praktische Hinweise und Lösungen für typische Konfliktfälle.

David Herzog ist Fachanwalt für Steuerrecht sowie Handels- und Gesellschaftsrecht und seit 2013 Lehrbeauftragter für Recht an der Hochschule Mannheim, Fakultät für Gestaltung.

[Leseprobe auf ISSUU.com](https://www.issuu.com/avedition)

avedition GmbH
Verlag für Architektur und Design
Senefelderstr. 109
D-70176 Stuttgart
Tel.: +49 (0)711 / 220 22 79-0

Geschäftsführer:
Dr. Petra Kiedaisch, Bettina Klett
USt.Id.: DE292753709
Amtsgericht Stuttgart
HRB Nummer: 747066