# Rechtssicherheit im Testdatenmanagement

Risiken vermeiden, Effizienz steigern


MENSCHEN MIT LÖSUNGEN

**Christoph Knopp** hat an der Goethe-Universität Frankfurt am Main Informatik studiert und arbeitet als Consultant im Bereich Testdaten-Management bei der GFB EDV Consulting und Services GmbH.

Christoph.Knopp@gfb-consulting.de

**Andreas Jaspers (Rechtsanwalt)** Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., einer der größten Fachverbände der Informations- und Kommunikationsbranche. Die GDD unterstützt Unternehmen bei der Lösung von technischen, rechtlichen und organisatorischen Fragen im Zusammenhang mit Datenschutz/ Datensicherheit.

## Datenschutzrechtliche Anforderungen nach Bundesdatenschutzgesetz und neuem EU-Datenschutzrecht

Die neue EU Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 gilt, erhöht die datenschutzrechtlichen Anforderungen beim Test von IT-Systemen. Insbesondere der erheblich erhöhte Sanktionsrahmen von bis zu 4 % des Vorjahresumsatzes gibt dringend Veranlassung, bei der Implementierung von IT-Systemen und Datenbanken den Datenschutz zu beachten.

Aber auch nach heutiger Rechtslage auf Grundlage des Bundesdatenschutzgesetzes ist es nicht erlaubt, personenbezogene Echtdaten ohne Beachtung des Datenschutzes zu Testzwecken zu verwenden. Trotzdem ist die Verwendung von Echtdaten beim Testen der Software nicht nur in der Integrationsphase sondern auch in der Testphase oftmals gängige, aber gefährliche und rechtswidrige Praxis.


## IMPRESSUM

**Herausgeber & Redaktion:**

GFB EDV Consulting und Services GmbH
Obere Zeil 2, 61440 Oberursel

Geschäftsführer: Andreas Günther
Michael Völker
Peter Laggner

HRB: 5878 Amtsgericht Bad Homburg

Michael Völker (V.i.S.d.P.)

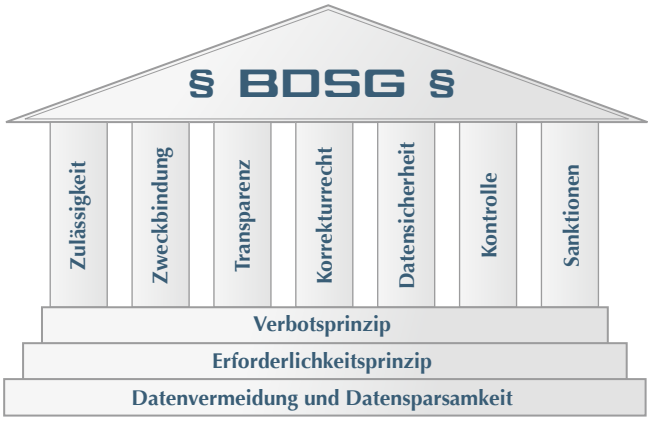
Kontakt: info@gfb-consulting.de
Tel.: +49 (0) 6171 5060-60
Fax: +49 (0) 6171 5060-66

Bildrechte:
Titel: © Chlorophylle - fotolia.com
© jpgon - Fotolia.com
S6/7: © mizar_21984 - fotolia.com
S8: © fotomek - fotolia.com
S8: © Fiedels - fotolia.com
S12: © blackred - istockphoto.com

## Datenschutzrisiken

Im Allgemeinen haben wesentlich mehr Personen Zugriff auf Testsysteme als im regulären Betrieb, da dort verschiedenste Tests, auch mit anderer Software und anderen Daten, durchgeführt werden. Der Zugriff von nicht Berechtigten kann somit nicht ausgeschlossen werden und birgt dementsprechende Missbrauchsgefahren. Die Datensicherheit kann durch die Verwendung unterschiedlicher Softwarestände gefährdet werden, da durch die Anzahl der Testversionen auch die Anzahl eventueller Fehlerquellen steigt. Falls Backups nicht im erforderlichen Maße durchgeführt werden, können versehentlich veränderte Daten nicht mehr rekonstruiert werden. Ein weiteres Missbrauchsrisiko besteht in der Versendung der Daten an Dritte zur Fehleranalyse, die den Kreis der Datennutzer noch einmal wesentlich erweitert.

## Enger Rahmen des Datenschutzrechts




Personenbezogene Daten dürfen nach dem Bundesdatenschutzgesetz (BDSG) grundsätzlich nur zweckgebunden, d.h. nur für die Zwecke genutzt werden, für die sie erhoben wurden. Die Nutzung der Daten ist also nur für die Erfüllung der jeweiligen Vertragszwecke gestattet, z.B. eines Kauf- oder Arbeitsvertrages.

Der Nutzung von Echtdaten für Testzwecke stellt eine Zweckänderung dar. Ausnahmsweise ist auch eine zweckändernde Nutzung zulässig. Diese ist nach der Vorgabe des BDSG nur dann zulässig, wenn dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist, zudem kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Nutzung überwiegt.

Im Rahmen dieser Interessenabwägung ist bereits zweifelhaft, ob die Nutzung von personenbezogenen Echtdaten zu Testzwecken erforderlich ist. Eine solche Erforderlichkeit ist zu verneinen, wenn auch ohne Echtdaten in geeigneter Weise getestet werden kann, z.B. durch Anonymisierung oder Pseudonymisierung mittels geeigneter Softwarelösungen.

Bei der Beurteilung entgegenstehender Betroffeneninteressen ist neben den vorgenannten Datenschutzrisiken zu prüfen, welche Sensibilität die zum Test vorgesehenen Datenkategorien haben. So sind reine Basisdaten (Name, Adresse) in der Regel weniger sensibel als detaillierte Kundeninformationen, wie gekaufte Artikel, Zahlungsrückstände etc.

Deutlich strengere Rechtsvorschriften finden mit Geltung der EU-Datenschutz-Grundverordnung (DSGVO) Anwendung. Ab dem 25.05.2018 ist eine Zweckänderung von Daten nur unter strengen Voraussetzungen zulässig. Für die Nutzung von personenbezogenen Daten für Testzwecke fordert die DSGVO in Artikel 6 Absatz 4 das „Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann“. Eine Nutzung von Echtdaten für Testzwecke, insbesondere im Projektbetrieb ist danach nicht zulässig. Als Lösung für die Migration beim Testen von Software bietet die DSGVO damit ausdrücklich die Pseudonymisierung an. Eine weitere Garantie könnte durch den Einsatz synthetischer Datensätze geschaffen werden.

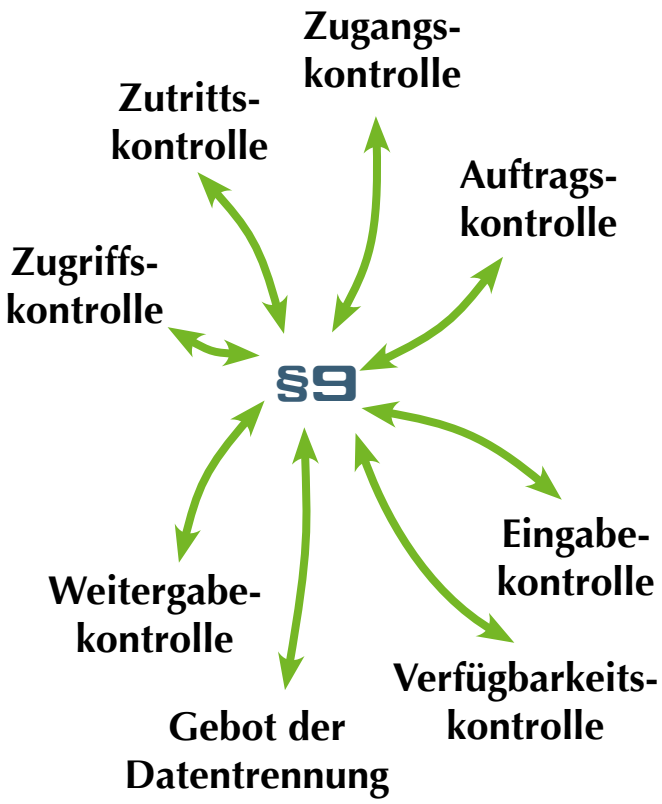
## Besonders sensible personenbezogene Daten

Nach dem BDSG und der DSGVO unterliegt die Verarbeitung besonders sensibler personenbezogenen Daten sehr strengen Zulässigkeitsvoraussetzungen. Betroffen sind Daten über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben. Diese Daten finden sich regelmäßig in Personalinformationssystemen aber auch im Versicherungs- und Bankenbereich. **Deren Verarbeitung kann nicht auf eine Interessenabwägung gestützt werden. Damit ist die Nutzung jedenfalls im Projektbetrieb für Funktionstests ausgeschlossen.**

## Datenvermeidung und Datensparsamkeit

Das BDSG fordert als grundlegendes Prinzip des Datenschutzes die Datenvermeidung und Datensparsamkeit. Die Verarbeitung personenbezogener Daten und die Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich - so der Wortlaut des BDSG - an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Personenbezogenen Daten sind zu anonymisieren bzw. pseudonymisieren, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Klassisches Anwendungsszenarium dieser Norm sind Funktions- und Programmtests. Die Beachtung des Prinzips der Datenvermeidung drängt die Frage nach geeigneten Softwarelösungen auf, mit der sich die Nutzung von Testdaten vermeiden lässt.

Die DSGVO erhöht diese Anforderung. Art. 25 Absatz 1 DSGVO fordert geeignete technische und organisatorische Maßnahmen, wie die Psydonymisierung, um den Datenschutzgrundsatz der Datenminimierung umzusetzen (Data protection by design). Auch diese Regelung ist nach der DSGVO bußgeldbewährt.




Die 8 Gebote der Datensicherheit
(BDSG §9 und Anlage)

## Datensicherheit

Neben den mit Blick auf die Nutzung von Testdaten restriktiven Zulässigkeitsrahmen hat das BSDG auch Vorgaben zum technischen und organisatorischen Datenschutz, die auch das Testen von Software und Systemen betreffen.
Nach der Anlage zu § 9 BDSG haben Unternehmen unter anderem zu gewährleisten, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle) sowie personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle). Damit fordern die technischen und organisatorischen Maßnahmen des § 9 BDSG eine Trennung von Produktiv- und Testsystem. Eine Lösung ist damit nicht das Testen im Livebetrieb. Als Konsequenzen für den Testbetrieb muss der Einsatz von personenbezogenen Echtdaten auch unter dem Gesichtspunkt der Datensicherheit als grundsätzlich unzulässig beurteilt werden, da er nicht nur eine Zweckdurchbrechung darstellt sondern auch die Integrität und die Vertraulichkeit der Daten gefährdet. Die Anforderungen an Ausnahmen sind sehr hoch zu setzen, z.B. wenn das System eine solche Komplexität aufweist, dass ohne Echtdaten nicht aussagekräftig getestet werden kann. Allerdings sind hier immer die Möglichkeiten moderner Softwarelösungen zur Anonymisierung oder Pseudonymisierung zu berücksichtigen.
Die Nachfolgereglung in Art. 32 DSGVO verlangt ein risikoadäquates Sicherheitskonzept. Maßgabe ist der Stand der Technik. Dieses fordert u.a. die Pseudonymisierung und Verschlüsselung als Bestandteil des Sicherheitskonzepts. Dieses muss zudem die Fähigkeit haben, die Vertraulichkeit zu gewährleisten. Diese Ziele sind bußgeldbewährt beim Test von IT-Systemen zu berücksichtigen.

## Informationspflichten bei Datenpannen

Je nach Art der Testumgebung und des Testverfahrens kann das Risiko bestehen, dass durch Systemfehler beim Testen mit Echtdaten ungeplant personenbezogenen Daten an Dritte übermittelt werden. Sind diese Daten besonders sensibel oder handelt es sich um Bank-oder Kreditkartendaten muss über diesen Datenverlust nach dem BDSG die Datenschutzaufsichtsbehörde und die Betroffenen informiert werden. Dies kann mit Imageverlusten für das Unternehmen verbunden sein. Nach Geltung der DSGVO muss sogar ungeachtet der Sensibilität innerhalb von 72 Stunden jeder Datenverlust der Aufsichtsbehörde gemeldet werden. Dieses Risiko lässt sich auch nach dem Wortlaut der DSGVO vermeiden, wenn ein Sicherheitskonzept die Verschlüsselung von Daten vorsieht.

## Datenschutz - Folgenabschätzung

Ein neues Instrument der Datenschutzorganisation eines Unternehmens ist die Datenschutz-Folgenabschätzung. Bei Verwendung neuer Technologien, die besonderen Risiken für die Betroffenen aufweisen, hat das Unternehmen gemäß Artikel 35 DSGVO eine Abschätzung der Folgen vorzunehmen. Insbesondere wenn besonders sensible Daten verarbeitet werden sollen, bedarf es bei der Planung der Tests von IT-Systemen einer Analyse der Risiken auf technologischer Ebene, die ggfls. mittels Pseudonymisierung oder dem Einsatz synthetischer Datensätze minimiert oder ausgeschlossen werden können.

# Quick Check Datenschutz

## Echtdaten im Softwaretest

Nutzt ihr Unternehmen Echtdaten im Softwaretest, ohne diese zu anonymisieren oder pseudonymisieren? Falls ja, dann hilft Ihnen folgende Checkliste dabei festzustellen, ob Sie dabei auch den Datenschutz einhalten. Bei einen bis zwei offenen Punkten sollten Sie diese mit einem Datenschutzexperten abklären. Sollten Sie mehrere Punkte nicht erfüllen können, besteht akuter Handlungsbedarf.

1. Wurden im Vorfeld ausgiebige Tests ohne Echtdaten durchgeführt? ☐ JA ☐ NEIN
2. Werden die Echtdaten nur im Rahmen zusätzlicher, minimierter Tests verwendet und finden diese nur in einer definierten und kontrollierten Umgebung statt? ☐ JA ☐ NEIN
3. Es existiert keine bereichsspezifische Rechtsvorschrift, die den Test mit Echtdaten ausdrücklich untersagt? ☐ JA ☐ NEIN
4. Liegen Fehler aus dem Produktionsbetrieb vor, die sich ohne Echtdaten nicht aufklären lassen? ☐ JA ☐ NEIN
5. Wäre die Anonymisierung der Echtdaten mit unvertretbar hohem Aufwand verbunden? ☐ JA ☐ NEIN
6. Hat die verantwortliche Stelle dem Test mit Echtdaten schriftlich zugestimmt (Geschäftsleitung)? ☐ JA ☐ NEIN
7. Wurde vorab der betriebliche oder behördliche Datenschutzbeauftragte informiert? ☐ JA ☐ NEIN
8. Wird bei der Durchführung und Auswertung der Tests die schutzwürdigen Belange der Betroffenen und die Datensicherheit berücksichtigt? ☐ JA ☐ NEIN
9. Haben nur solche Personen auf die Echtdaten Zugriff, welche auch für die Fehlerbehebung und Durchführung der Test erforderlich sind? ☐ JA ☐ NEIN
10. Unterliegen diese Personen den jeweils maßgebenden Vertraulichkeitsgrundsätzen und insbesondere datenschutzrechtlichen Vorschriften? ☐ JA ☐ NEIN
11. Wurde der Zugriff auf die Echtdaten protokolliert und die Verwendung mit Anlass, Begründung, Umfang und Dauer, die getroffenen Sicherheitsmaßnahmen sowie die vorangegangen Tests mit Testdaten revisionssicher dokumentiert? ☐ JA ☐ NEIN
12. Sind die Kurzfassung eines IT-Konzeptes sowie ein auf die Testbedingungen angepasstes Sicherheitskonzept vorhanden? ☐ JA ☐ NEIN

**Bei einen bis zwei „Nein" sollten Sie diese mit einem Datenschutzexperten abklären. Sollten Sie mehrere Punkte nicht erfüllen können, besteht akuter Handlungsbedarf.**

# Orientierungshilfe der Datenschutz-Aufsichtsbehörden

Die Datenschutz-Aufsichtsbehörden fordern in einer Orientierungshilfe „Datenschutz und Datensicherheit in Projekten[1]" eine Differenzierung zwischen Projekt- und Produktivbetrieb. **Für den Projektbetrieb sollen bei Funktions- und Integrationstests grundsätzlich keine personenbezogenen Echtdaten genutzt werden dürfen.** Zudem bedarf es einer Kurzfassung eines IT-Konzepts sowie eines auf die Testbedingungen angepassten Sicherheitskonzepts. Auch für den Produktivbetrieb wird ein Sicherheitskonzept gefordert. Notwendige Tests mit Echtdaten sollten sich auf Daten von Personen beschränken, die für das Verfahren verantwortlich oder Mitarbeiter des Projekts sind und diesen Tests zugestimmt haben. Zudem wird die Freigabe für den Produktivbetrieb durch die Unternehmensleitung gefordert, wohl um die datenschutzrechtliche Verantwortlichkeit zu unterstreichen.

# Konsequenzen von Datenschutz-verstößen

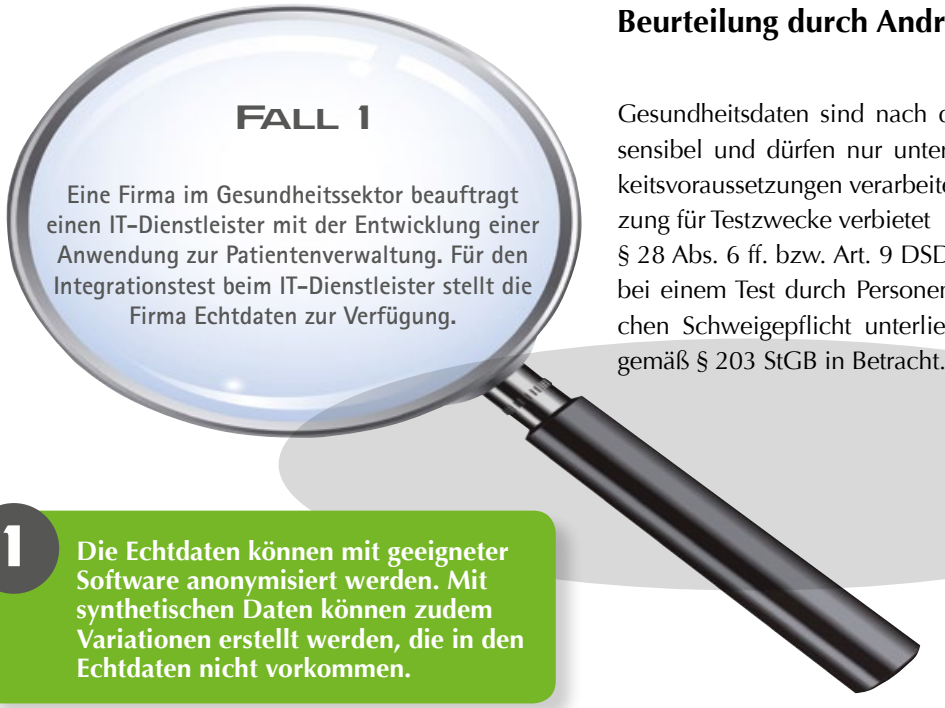
Datenschutzverstöße können ein Einschreiten der Datenschutz-Aufsichtsbehörden zur Folge haben. Diese können Bußgelder bis zu 300.000,- € verhängen sowie Auflagen für die System – und Programmtests erteilen. Die DSGVO hat einen erheblich verschärften Bußgeldrahmen. Danach können Bußgelder bis zu 20 Millionen Euro oder bis zu 4 % des weltweiten (Konzern-) Jahresumsatzes, je nachdem welcher der Beträge höher ist, verhängt werden. Dabei müssen die verhängten Bußgelder „wirksam, verhältnismäßig und abschreckend sein".

Datenverluste können zudem Strafbewährungen erfüllen wie die Verletzung von Amts-, Berufs- und Privatgeheimnissen, die Verletzung des Post- oder Fernmeldegeheimnisses oder Verrat von Geschäfts- und Betriebsgeheimnissen.

Bei Verlusten von sensiblen Daten oder Daten zu Kredit- und Bankkonten auf Grund sicherheitstechnisch unzulänglicher System- und Programmtests sind nach einer Risikobeurteilung zudem auch die Aufsichtsbehörden und die Betroffenen hiervon zu informieren. Der Imageverlust des Unternehmens ist dabei sicherlich der größte Schaden.

1) www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OH_Projekt-Produktivbetrieb.pdf

# Beispiele aus der Praxis




## Beurteilung durch Andreas Jaspers

Gesundheitsdaten sind nach dem BDSG besonders sensibel und dürfen nur unter restriktiven Zulässigkeitsvoraussetzungen verarbeitet werden. Deren Nutzung für Testzwecke verbietet
§ 28 Abs. 6 ff. bzw. Art. 9 DSDVO. Daneben kommt bei einem Test durch Personen, die nicht der ärztlichen Schweigepflicht unterliegen, eine Strafbarkeit gemäß § 203 StGB in Betracht.

**1** **Die Echtdaten können mit geeigneter Software anonymisiert werden. Mit synthetischen Daten können zudem Variationen erstellt werden, die in den Echtdaten nicht vorkommen.**


## Beurteilung durch Andreas Jaspers

Die Übermittlung von Gesundheitsdaten vom Arzt zum Softwareanbieter zu Testzwecken ist datenschutzrechtlich unzulässig und sogar gemäß § 203 StGB strafbewehrt (Verletzung der ärztlichen Schweigepflicht!).

**2** **Fall A: Die Daten werden beim Kunden vor der Übermittlung komplett oder selektiv in eine andere Datenbank anonymisiert.**
**Fall B: Beim Remote Zugriff werden die Daten vor der Anzeige anonymisiert dargestellt (Live Anonymisierung).**

# Beispiele aus der Praxis

## Fall 3

Ein Dienstleistungsunternehmen beauftragt einen Entwickler im EU-Ausland damit, die Anwendung für die Vertrags- und Kundenverwaltung neu zu programmieren. Für den Softwaretest erhält der Entwickler regelmäßig einen anonymisierten Abzug der Echtdaten. Treten Fehler in der Produktion auf, die auf Grund der Anonymisierung nicht nachgestellt werden können, werden die Echtdaten des betroffenen Datensatzes an den Entwickler übermittelt.

### Beurteilung durch Andreas Jaspers

Bei Übermittlung von personenbezogenen Daten zu Testwecken in Drittländer ist zweistufig zu prüfen. Zunächst muss die Übermittlung von Echtdaten überhaupt erforderlich sein, was mit Blick auf deren Sensibilität in der Regel problematisch ist. Bei einer Übermittlung in das EU-Ausland muss zusätzlich beim Empfänger ein angemessenes Datenschutzniveau vorliegen oder sehr aufwendig vertraglich geregelt werden. Eine Anonymisierung der Daten für Testzwecke vor deren Übermittlung nimmt die datenschutzrechtliche Brisanz.

**3** **Mit geeigneter Software können die Echtdaten so anonymisiert werden, dass vorhandene Defekte mit hoher Wahrscheinlichkeit erhalten bleiben.**

## Fall 4

Für den Integrationstest einer Anwendung, die über mehrere Systeme verteilt ist, wird eine gemeinsame Testumgebung aufgebaut. Aus den Echtdaten werden für den Test geeignete Vertragsnummern ermittelt. Diese Auswahl wird anonymisiert in die Testumgebung übertragen, die Vertragsnummern werden beibehalten, um diese den Testfällen zuordnen zu können.

### Beurteilung durch Andreas Jaspers

Ein personenbezogenes Datum i.S.d. BDSG bzw, der DSGVO liegt bereits vor, wenn Daten einer Person zugeordnet werden können. Dies ist über die Vertragsnummer der Fall. Damit liegt bei Beibehaltung der Vertragsnummer im Testverfahren keine rechtskonforme Anonymisierung vor.

**4** **Bereits bei Auswahl der geeigneten Vertragsnummern müssen diese anonymisiert sein (z.B. durch Vertauschung).**

### Beurteilung durch Andreas Jaspers

Die unzulässige Datenübermittlung hat zur Folge, dass gemäß § 42a BDSG bzw. Art. 33,34 DSGVO die betroffenen Bankkunden, deren Kreditkartendaten fehlerhaft Dritten übermittelt wurden, über diesen Vorfall informiert werden müssen. Zugleich müssen Empfehlungen zur Vermeidung und Aufdeckung eines Missbrauchs unterbreitet werden. Diese Informationen sind auch der zuständigen Datenschutzaufsichtsbehörde mitzuteilen.

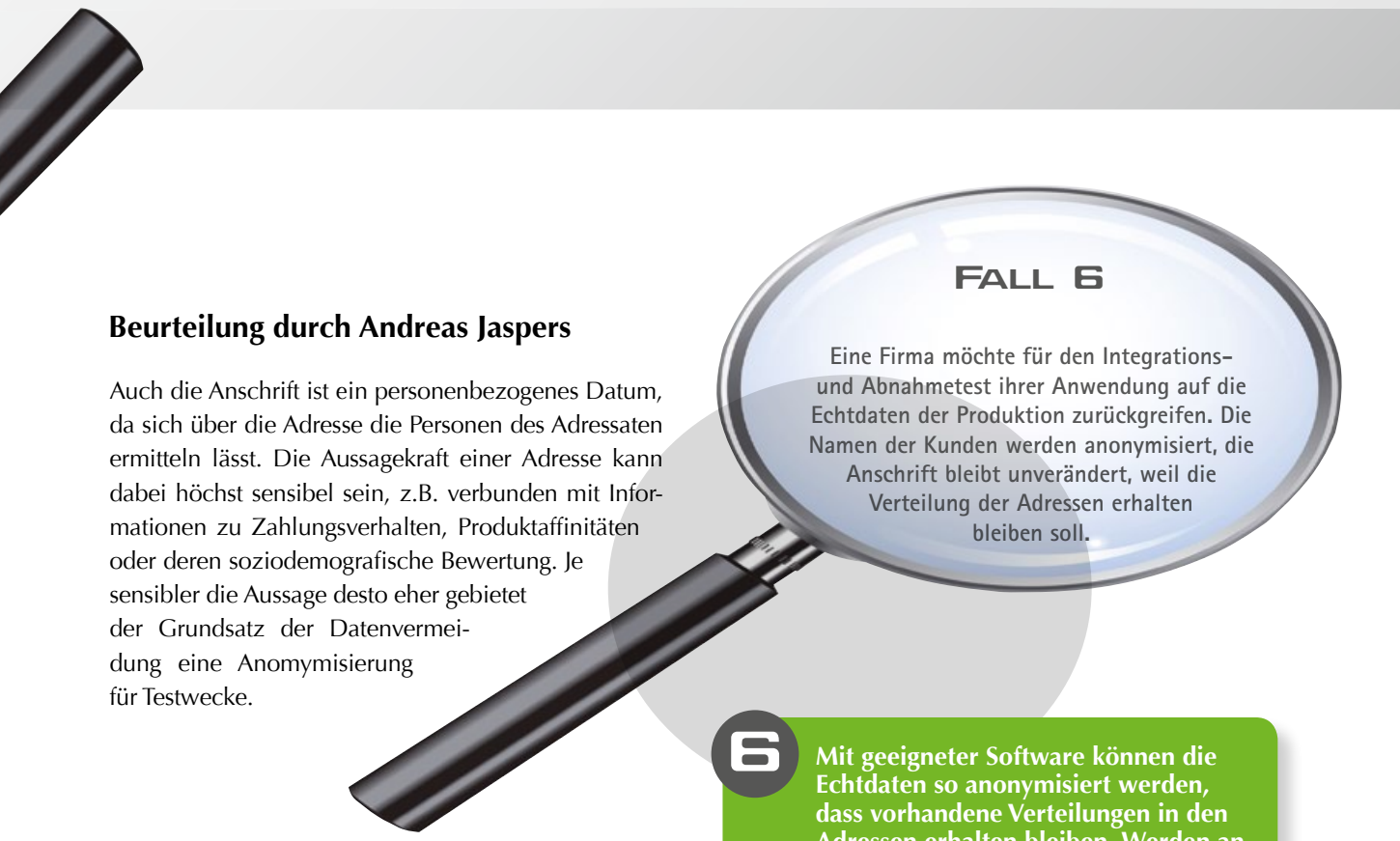
## Fall 5

Eine Bank stellt beim Test mit Echtdaten fest, dass aufgrund einer Sicherheitslücke Kreditkartenabrechnungen von Kunden an falsche Empfänger übermittelt worden sind.

**5** **Ein Sicherheitskonzept muss vor der Testphase jede Datenpanne ausschließen. Dazu gehört auch die Verwendung von pseudonymisierten Daten für Testzecke.**

## Beurteilung durch Andreas Jaspers

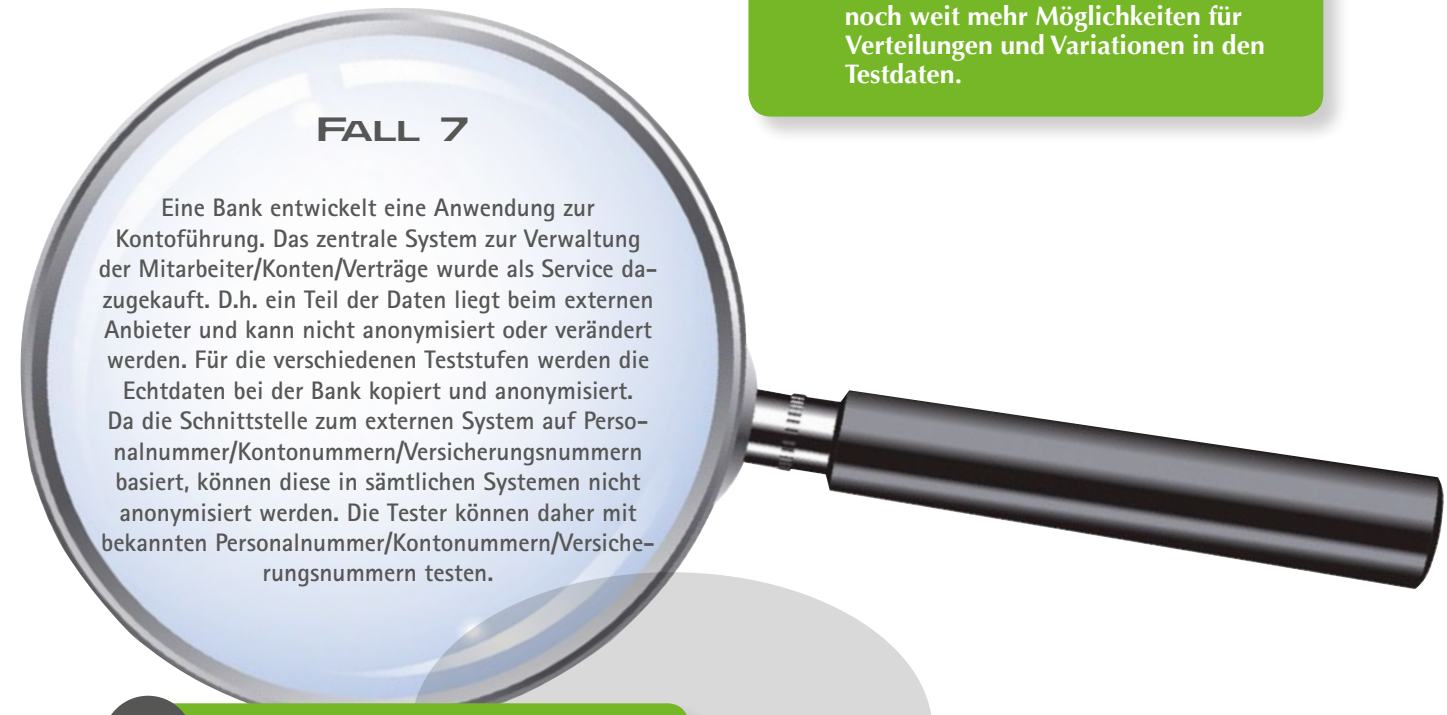
Auch die Anschrift ist ein personenbezogenes Datum, da sich über die Adresse die Personen des Adressaten ermitteln lässt. Die Aussagekraft einer Adresse kann dabei höchst sensibel sein, z.B. verbunden mit Informationen zu Zahlungsverhalten, Produktaffinitäten oder deren soziodemografische Bewertung. Je sensibler die Aussage desto eher gebietet der Grundsatz der Datenvermeidung eine Anomymisierung für Testwecke.



### Fall 6

Eine Firma möchte für den Integrations- und Abnahmetest ihrer Anwendung auf die Echtdaten der Produktion zurückgreifen. Die Namen der Kunden werden anonymisiert, die Anschrift bleibt unverändert, weil die Verteilung der Adressen erhalten bleiben soll.

**6** **Mit geeigneter Software können die Echtdaten so anonymisiert werden, dass vorhandene Verteilungen in den Adressen erhalten bleiben. Werden andere Verteilungen gewünscht, können auch diese hergestellt werden. Synthetische Daten bieten darüber hinaus noch weit mehr Möglichkeiten für Verteilungen und Variationen in den Testdaten.**



### Fall 7

Eine Bank entwickelt eine Anwendung zur Kontoführung. Das zentrale System zur Verwaltung der Mitarbeiter/Konten/Verträge wurde als Service dazugekauft. D.h. ein Teil der Daten liegt beim externen Anbieter und kann nicht anonymisiert oder verändert werden. Für die verschiedenen Teststufen werden die Echtdaten bei der Bank kopiert und anonymisiert. Da die Schnittstelle zum externen System auf Personalnummer/Kontonummern/Versicherungsnummern basiert, können diese in sämtlichen Systemen nicht anonymisiert werden. Die Tester können daher mit bekannten Personalnummer/Kontonummern/Versicherungsnummern testen.

**7** **Falls das externe System nicht ebenfalls anonymisiert werden kann, erfolgt eine Anonymisierung der Schnittstelle. Innerhalb der Testumgebung haben die Tester nur Zugriff auf die anonymisierten Personalnummern/Kontonummern/Versicherungsnummern. Mit geeigneter Software findet für die Schnittstelle eine Transformation auf die realen Personalnummern/Kontonummern/Versicherungsnummer statt, die nur innerhalb der Software verfügbar ist.**

## Beurteilung durch Andreas Jaspers

Da es sich bei der Datenverarbeitung des Diensteisters um eine Auftragdatenverarbeitung handelt, bleibt die Bank datenschutzrechtlich verantwortlich. Diese ist neben der Beachtung des Datenschutzes auch zur Wahrung des Bankgeheinmisses verpflichtet. Vor diesem Hintergrund empfiehlt sich bei einer Bank regelmäßig eine Anonymisierung der Kundendaten zu Testzwecken.

## Zusammenfassung

- Vor dem Test bedarf es einer Kurzfassung eines IT-Konzepts sowie eines auf die Testbedingungen angepassten Sicherheitskonzepts.
- Die Verwendung von Echt- bzw. Produktivdaten ist strengestens verboten. Ein Verstoß kann mit bis zu 4% des weltweiten (Konzern-) Jahresumsatzes geahndet werden.
- Meldepflicht bei Datenpannen und Datenverlusten.

## Wir bieten Ihnen massgeschneiderte Lösungen

Mit einem perfekt auf die Größe und benötigten Bedarf Ihres Unternehmens abgestimmten Testdatenmanagement steht Ihr Unternehmen besser dar:

- Erhöhung der Datensicherheit
- Steigerung der Effizienz Ihrer IT
- Senkung der IT-Kosten
- Schnellere Bereitstellung von IT-Services
- Verbesserung der Informationsauswertung
- Optimierung der internen Zusammenarbeit
- Erhöhung der Kundenzufriedenheit
- Prozessoptimierung

# Wir sind Menschen mit Lösungen

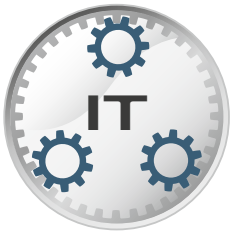
Die GFB EDV Consulting und Services GmbH ist ein inhabergeführtes, eigenfinanziertes und hochspezialisiertes Unternehmen mit ca. 20 festangestellten Mitarbeitern. Seit der Gründung im Jahre 1997 bringen wir uns ständig im Bereich neuer Technologien und Arbeitsweisen ein. Dadurch ist die GFB immer auf dem aktuellen Stand der Zeit. Tangentiale Technologien finden ebenso Berücksichtigung wie eine hohe technische Breite bei gleichzeitiger Spezialisierung in den Einzeldisziplinen. Das Unternehmen engagiert sich aktiv im ASQF.

GFB EDV Consulting und Services GmbH nutzt die Synergien ihrer drei Tätigkeitsfelder und liefert damit ihren Kunden hochwertige Dienstleistungen, Services und Produkte.

Weitere Informationen über die GFB EDV Consulting und Services GmbH
finden Sie unter www.gfb-consulting.de

GFB IT-Consulting & Services

## Consulting




Im Bereich IT-Consulting liefert die GFB innovatives Know-How und Technologien aus den Bereichen Softwareentwicklung, Qualitäts- und Systemmanagement.

**IT-Management ist mehr als Beratung**

- Testdatenmangement Beratung/ Umsetzung und Schulung
- Testumgebungsmanagement
- Q-up Implementierungen u. Schulung
- Qualitätssicherung
  - Testdurchführung/-automatisierung
  - Testplanung und Testdesign
- Buildmanagement
- Konfigurations- u. Release-Management
- Anforderungsmanagement
- Geschäftsprozessmodellierung
- Toolchain-Consulting

## Testdaten-management


Professionelles Testdatenmanagement (TDM) gewährt Ihrem Unternehmen Rechtssicherheit und deutliche Vorteile in der Qualitätssicherung.

**Unsere Methodik, unser Vorgehen**

Forschung, Entwicklung von Praxismodellen:

- GFB TDM-Vorgehensmodell©
- GFB TDM-6-Stufen-Modell©
- GFB TDM-Baukasten©
- GFB TDM-Cockpit©
- GFB TDM-Benchmark©

Darüber hinaus bieten wir die entsprechenden Schulungen, Zertifikate und IT-Consulting an.

## Der Testdaten-generator


Q-up – Der Testdatengenerator, seit 2010 erfolgreich in vielen Branchen im Einsatz, bündelt das praxisnahe Know-How aus den Bereichen IT-Consulting und Testdatenmanagement in Form von wiederverwendbaren und standardisierbaren Softwaremodulen.

**Unsere Produktfamilie**

- Anonymisierung
- Pseudonymisierung
- Synthetisierung
- Skalierung
- Automatisierung
- Testdatenreduktion
- Transformation
- Prozessabbildung
- Testumgebungsmanagement

# Mit unserem Testdatenmanagement sparen Sie 90% Zeit- und Personalkosten bei gleichzeitig höherer Datenqualität entsprechend der aktuellen Datenschutzbestimmungen

Microsoft Partner
Gold Independent Software Vendor (ISV)

## Rufen Sie an: +49 6171 5060-60

Telefonisch von Mo bis So von 6:30 Uhr – 22:00 Uhr
bzw. per Mail an **info@gfb-consulting.de**

**Bezugsquellen und Support:**

GFB EDV Consulting und Services GmbH
Obere Zeil 2
61440 Oberursel
Tel.: +49 (0) 6171 5060-60
Fax: +49 (0) 6171 5060-66
info@q-up-data.com
www.q-up-data.com

## Menschen mit Lösungen