



# Datenschutzmanagement- konzept

„Code of Conduct“ zum Schutz  
personenbezogener Daten

der  
dat repair GmbH  
Am Sophienhof 8-10  
24941 Flensburg  
Germany

Datum: 10.03.2009

## Inhaltsverzeichnis

Zweck des Code of Conduct.....	1
Rechtsgrundlagen & Code of Conduct .....	1
Grundsätze der Datenverarbeitung bei «dat repair» .....	2
Einwilligung.....	3
Besondere Arten personenbezogener Daten .....	3
Rechte der Betroffenen .....	4
Datengeheimnis & Vertraulichkeit .....	5
Datenverarbeitung im Auftrag .....	5
Datenschutzmanagement.....	6
Zusammenarbeit mit Aufsichtsbehörden .....	7
Technische und organisatorische Maßnahmen zum Datenschutz.....	7
Überprüfung des Datenschutzniveaus .....	9
Fortentwicklung des Code of Conduct .....	9

# Code of Conduct

## Zweck des Code of Conduct

Für die dat repair GmbH (nachfolgend: «dat repair») ist der Schutz personenbezogener Daten von höchster Bedeutung. Vertrauen in einen sicheren Umgang mit Daten von Kunden, Vertragspartnern und Dritten ist ein wesentliches Element in der Geschäftsphilosophie des Unternehmens.

Um Vertrauen und einen hohen Standard im Unternehmen zu erhalten und weiter auszubilden, soll dieser Code of Conduct dienen. Der Code of Conduct ist eine Leitlinie für den Datenschutz im Unternehmen. Ziel der Leitlinie ist es, einen einheitlichen Standard in den Bereichen Datenschutz und Datensicherheit bei der «dat repair» aufzustellen, der den hohen Anforderungen des deutschen Datenschutzrechts und auch den Vorgaben der Europäischen Datenschutzrichtlinie<sup>1</sup> entspricht.

Der Code of Conduct soll Führungskräften und Mitarbeitern bei kurz, mittel- und langfristigen strategischen Unternehmensentscheidungen eine Entscheidungshilfe sein.

## Rechtsgrundlagen & Code of Conduct

Dieser Code of Conduct soll ein hohes Datenschutzniveau bei «dat repair» gewährleisten.

Er ersetzt jedoch nicht die notwendige, im Einzelfall maßgebliche gesetzliche Befugnis zur Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch «dat repair» erfolgt auf Grundlage des Rechts der Bundesrepublik Deutschlands in Verbindung mit ggf. bestehenden vertraglichen Regelungen, die mit den jeweiligen Vertragspartnern von «dat repair» bestehen.

---

<sup>1</sup> Richtlinie 95/46/ EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

## Grundsätze der Datenverarbeitung bei «dat repair»

«dat repair» fühlt sich nachfolgenden Grundsätzen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten verpflichtet:

- Personenbezogene Daten werden nur erhoben, verarbeitet und genutzt, wenn eine gesetzliche Befugnisgrundlage besteht oder der Betroffene wirksam eingewilligt hat.
- Personenbezogene Daten werden nur für die Zwecke verarbeitet und genutzt, für die sie erhoben wurden. Eine Zweckänderung ist nur zulässig, wenn die gesetzlichen Voraussetzungen hierfür vorliegen.
- Persönlichkeitsrechte von Betroffenen müssen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gewahrt werden.
- Daten von Betroffenen sollen richtig und - falls erforderlich - aktuell sein. Es muss gewährleistet sein, dass nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden.
- Daten, die nicht mehr für den Geschäftszweck, für den sie ursprünglich erhoben wurden, erforderlich sind, werden unverzüglich gelöscht, sofern und soweit nicht gesetzliche Aufbewahrungspflichten bestehen.
- Eine Nutzung personenbezogener Daten für Werbe- oder Marketingzwecke erfolgt nur bei Vorliegen einer Einwilligung des Betroffenen.
- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten hat sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen (Grundsatz der Datenvermeidung und Datensparsamkeit)
- Bei der Planung neuer IT-Systeme und IT-Verfahren, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte von «dat repair» frühzeitig zu beteiligen.
- Es werden die zum Schutz personenbezogener Daten und zur Datensicherheit erforderlichen technischen und organisatorischen Maßnahmen getroffen.

- Der Datenschutzbeauftragte ist Ansprechpartner der Unternehmensleitung und Mitarbeiter und berät bei der Anwendung der einschlägigen datenschutzrechtlichen Vorgaben.

## Einwilligung

Sofern die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten nicht schon auf Grundlage einer gesetzlichen Befugnis besteht, wird spätestens bei der Datenerhebung eine Einwilligung vom Betroffenen eingeholt.

«dat repair» wird den Betroffenen vor Einholung der Einwilligung in transparenter und umfassender Weise, über Zweck, Art und Umfang der beabsichtigten Verwendung der Daten informieren.

Die Einwilligung muss ausdrücklich und freiwillig erfolgen. Sofern die Verweigerung der Einwilligung Konsequenzen für den Betroffenen hat, wird dieser auf die Folgen der Verweigerung hingewiesen werden.

«dat repair» wird Sorge dafür tragen, dass die Informationen, die im Zusammenhang mit der Abgabe von Einwilligungserklärungen stehen, in verständlicher Form für den Betroffenen zur Verfügung stehen.

Die Abgabe einer Einwilligung kann schriftlich oder elektronisch erfolgen. In Ausnahmefällen kann die Einwilligung auch mündlich erfolgen. «dat repair» soll in diesen Fällen die besonderen Umstände, die die mündliche Einwilligung angemessen erscheinen lassen, dokumentieren.

## Besondere Arten personenbezogener Daten

Die Erhebung, Verarbeitung und Nutzung von Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (besondere Arten personenbezogener Daten) ist grundsätzlich untersagt, sofern sich die Befugnis zur Erhebung, Verarbeitung oder Nutzung nicht aus einer gesetzlichen Erlaubnis oder einer gesetzlichen Verpflichtung ergibt.

Eine Verwendung besonderer Arten personenbezogener Daten ist ferner zulässig im Falle von außergerichtlichen oder gerichtlichen Auseinandersetzungen, sofern kein Grund zu der Annahme besteht, dass das schutzwürdi-

ge Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ansonsten soll eine Einwilligung des Betroffenen eingeholt werden.

## Rechte der Betroffenen

Betroffene können sich jederzeit mit Fragen und ggf. Beschwerden an den Datenschutzbeauftragten von «dat repair» wenden.

- Der Betroffene kann Auskunft verlangen über die zu seiner Person gespeicherten Daten, den Zweck der Speicherung und ggf. deren Herkunft.
- Sofern Daten des Betroffenen an Dritte weitergegeben worden sind, hat der Betroffene Anspruch auf Auskunft über die Identität der Empfänger bzw. Kategorien der Empfänger.
- Sofern Daten des Betroffenen sich als unrichtig herausstellen, hat der Betroffene ein Berichtigungsrecht und «dat repair» wird die personenbezogenen Daten korrigieren.
- Sofern sich bei einer Überprüfung herausstellt, dass der Zweck der Datenverarbeitung durch Zeitablauf oder andere Gründe entfallen ist, wird «dat repair» die betreffenden Daten löschen. Etwasige gesetzliche Aufbewahrungspflichten bleiben unberührt.
- Der Betroffene hat das Recht, der Nutzung seiner personenbezogenen Daten zu Zwecken der Direktwerbung oder der Markt- und Meinungsforschung zu widersprechen. Für diese Zwecke wird «dat repair» die Daten in geeigneter Weise sperren.
- Der Betroffene hat darüber hinaus ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner personenbezogenen Daten. Für den Fall, dass eine Prüfung ergibt, dass ein schutzwürdiges Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das rechtmäßige Interesse von «dat repair» überwiegt, wird «dat repair» die betreffenden Daten löschen oder sperren, sofern nicht eine gesetzliche Verpflichtung zur Datenverarbeitung besteht.

## Datengeheimnis & Vertraulichkeit

Eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur den Mitarbeitern erlaubt, die auf die Einhaltung des Datengeheimnisses besonders verpflichtet wurden.

«dat repair» trägt Sorge dafür, dass alle Mitarbeiter bei Begründung des Arbeitsverhältnisses entsprechend ihrer Tätigkeit auf das Datengeheimnis, das Fernmeldegeheimnis und auf ein etwaiges Recht von Betroffenen auf den Schutz von Vertraulichkeit und Integrität von IT-Systemen verpflichtet werden.

Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

## Datenverarbeitung im Auftrag

Sofern ein anderes Unternehmen als „Subunternehmer“ Dienstleistungen für «dat repair» erbringt und in diesem Zusammenhang auch personenbezogene Daten erhoben, verarbeitet und genutzt werden, trägt «dat repair» Sorge dafür, dass der „Subunternehmer“ sorgfältig ausgewählt wird und die Auswahl sich insbesondere an dem Aspekt des Schutzes personenbezogener Daten orientiert.

«dat repair» wird den Auftragnehmer verpflichten, die gesetzlichen Vorgaben zum Schutz personenbezogener Daten zu treffen und insbesondere auch auf Anfrage nachzuweisen, dass die Mitarbeiter, die im Rahmen der Erbringung von Leistungen für «dat repair» tätig werden, auf das Datengeheimnis verpflichtet wurden.

«dat repair» wird schriftliche Weisungen bezüglich Art, Zweck und Umfang der Verarbeitung personenbezogener Daten an den Auftragnehmer erteilen und die Einhaltung der Vorgaben ggf. durch Kontrollen sicherstellen.

Sofern «dat repair» selbst im Wege der Auftragsdatenverarbeitung Leistungen durch Subunternehmer erbringen lassen will, wird zuvor eine Genehmigung vom Auftraggeber als verantwortliche Stelle für das Unterauftragsver-

hältnis eingeholt werden, sofern nicht bereits eine Genehmigung erteilt wurde.

## Datenschutzmanagement

«dat repair» fühlt sich dem Datenschutz und der weiteren Entwicklung des Datenschutz im Unternehmen verpflichtet. Um einen „lebendigen“ Datenschutz im Unternehmen zu gewährleisten, erfolgt eine frühzeitige Einbindung des Datenschutzbeauftragten bei der Vorbereitung von Unternehmensentscheidungen, sofern diese einen Bezug zur Verarbeitung personenbezogener Daten haben. Die Unternehmensleitung wird den Datenschutzbeauftragten bei der Ausführung seiner gesetzlichen Aufgaben und der Aufgaben aus diesem Code of Conduct unterstützen.

Der Datenschutzbeauftragte berät und unterstützt die Unternehmensleitung bei der Implementierung von Datenschutz und datenschutzfreundlichen Technologien im Zusammenhang mit der Einführung neuer Geschäftsprozesse.

Bestehende Geschäftsprozesse werden im Rahmen turnusmäßiger Überprüfungen auch unter Berücksichtigung datenschutzrechtlicher Aspekte evaluiert und angepasst.

Der Datenschutzbeauftragte von «dat repair» wird unverzüglich über Verstöße (auch schon bei Verdacht auf Verstöße) gegen datenschutzrechtliche Verpflichtungen und diesen Code of Conduct informiert.

Der Datenschutzbeauftragte und die Unternehmensleitung koordinieren im Zusammenwirken die künftige Datenschutzpolitik des Unternehmens. Der Datenschutzbeauftragte ist im Rahmen der Ausübung seiner gesetzlichen Aufgaben weisungsfrei.

«dat repair» trägt Sorge dafür, dass alle Mitarbeiter in erforderlichem Umfang über das Thema Datenschutz im Allgemeinen und Datenschutz bei «dat repair» im Besonderen unterrichtet werden. Mitarbeiter, deren Schwerpunkt die Verarbeitung personenbezogener Daten ist, sollen besonders geschult werden.

## Zusammenarbeit mit Aufsichtsbehörden

Im Falle einer anlassbezogenen oder nichtanlassbezogenen Kontrolle oder Anfrage durch die jeweils zuständige Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich, wird «dat repair» Anfragen innerhalb eines angemessenen Zeitraums sowie in einem zumutbaren Umfang zu antworten und Empfehlungen der Aufsichtsbehörde berücksichtigen.

Für den Fall, dass die Anfrage der Aufsichtsbehörde eine Verarbeitung betrifft, für die «dat repair» als Auftragsdatenverarbeiter tätig ist, wird «dat repair» die verantwortliche Stelle über die Anfrage der Aufsichtsbehörde informieren und das weitere Vorgehen abstimmen.

## Technische und organisatorische Maßnahmen zum Datenschutz

«dat repair» trifft die jeweils erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Zu diesen Maßnahmen gehören insbesondere:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle):
- insbesondere durch: gesicherte Eingänge, einbruchhemmende Fenster, Alarmanlage, Schlüsselkartensystem/Berechtigungsausweise (Interflex), Besucherlisten, Aufenthalt von Besuchern nur mit Begleitpersonen, Physische Gerätesicherungen
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):
- insbesondere durch: differenziertes Benutzerberechtigungskonzept, Rechte-/Rollenverwaltung auf ADS-Ebene, Authentifikation durch Benutzername/Passwort, sichere Passworte/Passwortwechsel, Sperrungen bei mehrfach fehlerhaften Zugangsversuchen, Einsatz von VPN, Virens Scanner, Trennung von Netzwerken (Werkstatt/Verwaltung)

- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):
  - insbesondere durch: Berechtigungskonzept, beschränkte Anzahl von Systemadministratoren, Protokollierung von Missbrauchsversuchen, Aufbewahrung von Datenträgern in gesicherten Räumen, ordnungsgemäße Vernichtung von Datenträgern/Akten
  
- zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle):
  - insbesondere durch: Einrichtung von 1:1-Verbindungen zwischen Gebäuden, Verschlüsselungsverfahren, sichere Transportbehälter, Erstellung von Begleitpapieren, Dokumentation der Datenempfänger und ggf. des Versandweges, Protokollierung von ausgehenden E-Mails (ERP)
  
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):
  - insbesondere durch: Datenerfassungsanweisungen (QM), Protokollierung von Datenerhebungen/-löschungen, Sicherung von Protokolldaten
  
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle):
  - insbesondere durch: sorgfältige Auswahl von Auftragnehmern, Verpflichtung des Auftragnehmers zu Datenschutz/Datensicherheit, Erteilung von schriftlichen Weisungen i.S.d. § 11 BDSG, Schutzmaßnahmen gegen Datenverlust, Beach-

tung des Grundsatzes der Datenvermeidung und Datensparsamkeit

- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle):
- insbesondere durch: Backup- und Recoverykonzept, USV, Klimaanlage, Schutzsteckdosenleisten, Rauchmelder, Feuerlöschgerät, getrennte Lagerung von Backup-Datenträgern, Notfallplan
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungsgebot):
- insbesondere durch: Mandantentrennung softwareseitig, ggf. physikalische Trennung

## Überprüfung des Datenschutzniveaus

Das Unternehmen «dat repair» wird dem Grundsatz Rechnung tragen, dass in regelmäßigen Abständen eine Überprüfung des Datenschutzniveaus im Unternehmen und die Einhaltung dieses Code of Conduct durchgeführt werden soll, um die Wirksamkeit und das Optimierungspotential der eingeführten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten zu überprüfen.

Das Datenschutzaudit kann intern durch den Datenschutzbeauftragten erfolgen. Dieser kann in Abstimmung mit der Unternehmensleitung auch eine externe Person oder ein externes Unternehmen mit dem Audit beauftragen bzw. mit dieser/diesem zusammen das Audit durchführen.

## Fortentwicklung des Code of Conduct

«dat repair» wird diesen Code of Conduct anlassbezogen oder in regelmäßigen Abständen im Hinblick auf seinen Anpassungsbedarf und seine Fortentwicklung prüfen. Der Datenschutzbeauftragte wird diese Aufgabe koordinieren und vorbereiten.

Eine Anpassung kann insbesondere erforderlich werden, wenn sich die maßgebenden Rechtsgrundlagen ändern und/oder neue Geschäftsprozesse eingeführt oder bestehende Prozesse ganz oder teilweise geändert werden.