
# Fremd- und Fernwartung

## Orientierungshilfe
## und
## Checkliste

Rel. 2.0.0
2009-03-12

Landesbeauftragter für den Datenschutz Niedersachsen

## Vorbemerkung

Die Abhängigkeit von einer funktionierenden Datenverarbeitung ist in vielen Branchen der Wirtschaft und der Verwaltung bereits so groß, dass der kurzfristige Ausfall der Datenverarbeitung Existenz bedrohend sein kann. Dieses Risiko sowie zunehmende Systemkomplexität und verteilte Systemarchitekturen führen dazu, dass immer mehr Anwender ihre Systeme nicht mehr selbst warten. Als Folge davon werden Verträge für Wartungsarbeiten und Systembetreuung durch externe Personen oder Stellen abgeschlossen – häufig mit dem Unternehmen, das das eingesetzte Verfahren entwickelt und vertrieben hat.
Bei Wartung und Systembetreuung wird unterschieden:

- **Arbeiten vor Ort**
  Der Wartungstechniker oder externe Systembetreuer führt seine Arbeiten unmittelbar an den Datenverarbeitungsanlagen vor Ort durch.
- **Wartungsarbeiten und Systembetreuung außer Haus**
  Die Datenverarbeitungsanlagen werden für Wartungsarbeiten oder Systembetreuungsaufgaben außer Haus gegeben (z.B. Konfiguration, Aufspielen von Softwareprodukten).
- **Fernwartung (Fernsteuerung)**
  Wartungstechniker bzw. Systembetreuer sind über spezielle Netzzugänge an den zu wartenden Rechner angeschlossen. Mit Programmen zur Fernwartung lassen sich Systeme auch fernsteuern. Schaltet sich der Wartungstechniker in eine Station ein, wird dort über das vorgehaltene Programm die Verbindung hergestellt. Dabei besteht für ihn die Möglichkeit, den Bildschirminhalt des entfernten Rechners einzusehen sowie Datensammlungen zu lesen und zu verändern. Auch ein Dateitransfer lässt sich durchführen. Mit Programmen zur Fernanalyse können Informationen über Netzwerkauslastung und –aktivität ausgewertet werden.

Durch externe Wartung und Systembetreuung verliert die Daten verarbeitende Stelle sehr schnell das notwendige Fachwissen über das eingesetzte technische System. Sie ist bald nicht mehr in der Lage, die Tätigkeit des externen Wartungspersonals im Einzelnen nachzuvollziehen. Viele Institutionen machen sich über diese Risiken der externen Wartung keine Gedanken.

## Datenschutz

Sind personenbezogene Daten betroffen und gehen keine spezialgesetzlichen Rechtsvorschriften vor[1], ist für Stellen der Wirtschaft das Bundesdatenschutzgesetz (BDSG) und für öffentliche Stellen des Landes Niedersachsen das Niedersächsische Datenschutzgesetz (NDSG) anzuwenden.
Fest steht:
**Die Daten verarbeitenden Stellen[2] tragen für externe Wartungs- und Systembetreuungsarbeiten die datenschutzrechtliche Verantwortung.**

Grundsätzlich sind die Regelungen zur Datenverarbeitung im Auftrag zu beachten[3].
Folgende **Datenschutzpflichten** sind besonders hervorzuheben:

- Die Wartung der Datenverarbeitungsanlagen durch externe Personen oder Stellen birgt zusätzliche Gefahren und Risiken; sie sollte nur dann gewählt werden, wenn eine eigene Wartung nur eingeschränkt oder gar nicht möglich ist.
- Externe Personen oder Stellen, die mit der Wartung oder Systembetreuung von Einrichtungen zur automatisierten Datenverarbeitung betraut sind, haben nach den Weisungen des Auftraggebers zu arbeiten. Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidbar ist. Ziel muss es sein, den Zugriff auf personenbezogene Daten weitest gehend aus-

[1] § 1 Abs. 3 BDSG / § 2 Abs. 6 NDSG
[2] § 3 Abs. 7 BDSG / § 3 Abs. 3 NDSG
[3] § 11 BDSG / § 6 NDSG

zuschließen. Hiervon darf nur abgewichen werden, wenn die Kenntnisnahme personenbezogener Daten im konkreten Einzelfall unerlässlich ist.
- Liegt eine Fernwartung durch ausländische Stellen vor, ist sicherzustellen, dass die jeweiligen Regelungen zur Übermittlung von personenbezogenen Daten an Stellen außerhalb der Bundesrepublik Deutschland[4] beachtet werden.
- Die Auftragnehmer haben die technischen und organisatorischen Maßnahmen nach § 9 BDSG bzw. § 7 NDSG zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen.

Allgemeine **Sicherungsziele** sind:

- Gewährleistung der Vertraulichkeit der Daten,
- Sicherstellung der Integrität der Daten,
- Gewährleistung der Authentizität der Daten,
- Gewährleistung der Authentifikation von Benutzern,
- Gewährleistung der sicheren Zustellung,
- Sicherstellung der Verfügbarkeit,
- Sicherstellung der Revisionsfähigkeit.

## Gefahren- und Risikoanalyse

Wartung und Systembetreuung durch externe Personen oder Stellen schafft Gefahren und Risiken für die erklärten Sicherungsziele. Konkrete Gefahren sind z.B.
- Für die Wartung wird ein weiterer Zugang zum Rechner geschaffen, über den sich Personen mit umfassenden Rechten anmelden können oder der als Zugang von Unbefugten missbraucht wird.
- Die Daten verarbeitende Stelle kann bei der Fernwartung nur begrenzt kontrollieren, welche Person tatsächlich die Wartung vornimmt, welche Daten übertragen werden und welche Sicherungsmaßnahmen beim Auftragnehmer getroffen worden sind.
- Das Wartungspersonal kann unter Umständen auf den gesamten Datenbestand zugreifen.
- Der Datenverkehr zwischen Rechner und Wartungsfirma kann unbefugt zur Kenntnis genommen oder manipuliert abgehört werden.

Auftraggeber haben grundsätzlich vor der Entscheidung, ob Wartungsarbeiten und Systembetreuung durch externe Personen oder Stellen durchgeführt werden, zu prüfen, ob und in welchem Umfang wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien Gefahren für die Rechte der Betroffenen verbunden sind[5]. Eine Beauftragung darf nur erfolgen, soweit derartige Gefahren durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können[6].

## Technische und organisatorische Maßnahmen

Eine ausreichend sichere Form der Wartung und Systembetreuung durch externe Personen oder Stellen wird dann erreicht, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen ausreichenden Schutz bieten. Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich nach der Sensibilität der verarbeiteten Daten (siehe Schutzstufenkonzept[7]) und nach der technischen Anbindung. Wird eine dieser Maßnahmen vernachlässigt, ist eine sichere Fernwartung nicht möglich.
Weitere Anregungen zur datenschutzgerechten Ausgestaltung der Wartung und der Systemverwaltung finden Sie unter der Internetadresse www.lfd.niedersachsen.de (z.B. datenschutzrele-

[4] §§ 4 b + c BDSG / § 14 NDSG
[5] Art. 20 EG-Datenschutzrichtlinie / § 7 Abs. 3 NDSG
[6] www.lfd.niedersachsen.de >Service-Angebote >Technische Hilfen >Vorabkontrolle
[7] www.lfd.niedersachsen.de >Service-Angebote >Technische Hilfen >Schutzstufen

vante Rechtsvorschriften, Empfehlungen, Orientierungshilfen, Checklisten sowie sonstige Materialien). Darüber hinaus bieten auch die IT-Grundschutzkataloge des BSI[8] wertvolle Hilfen.
Kann die Wartung und Systembetreuung durch externe Personen oder Stellen nicht ausreichend durch technische und organisatorische Maßnahmen gesichert werden, darf sie nicht in Anspruch genommen werden.

## Handlungsempfehlungen

Diese Orientierungshilfe hilft Gefahren und Risiken zu analysieren und gibt konkrete Empfehlungen für technische und organisatorische Sicherungsmaßnahmen.

Die Orientierungshilfe will
- Geschäfts- und Behördenleitung,
- Personalleitung und Personalvertretung,
- Systembetreuer,
- Datenschutzbeauftragter sowie
- Organisations- und DV-Leitung

in die Lage versetzen, ihr Konzept für eine datenschutzgerechte Wartung und Systembetreuung durch externe Personen oder Stellen zu entwickeln bzw. bestehende Lösungen zu überprüfen.

## Checkliste

Die folgende Checkliste konzentriert sich auf die Gesichtspunkte des technisch-organisatorischen Datenschutzes. Sie erhebt keinen Anspruch auf Vollständigkeit und ist im konkreten Einzelfall durch Zusatzfragestellungen zu ergänzen.

Die Checkliste unterteilt folgende Bereiche:
- Allgemeine Anforderungen
- Wartung und Systembetreuung vor Ort,
- Wartung und Systembetreuung außer Haus sowie
- Fernwartung.

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen
- Erfüllt
- Nicht erfüllt
- Trifft nicht zu

Diese Basisantworten können im Bedarfsfall durch kurze Erläuterungen in dem Feld Bemerkung ergänzt werden. Auf diese Weise liegt nach Durcharbeiten der Checkliste eine übersichtliche Aufstellung der zu treffenden Maßnahmen vor.

Alle als notwendig erachteten Maßnahmen sind in ein **Datensicherungskonzept** aufzunehmen und in regelmäßigen Abständen dahingehend zu prüfen, ob sie noch geeignet und angemessen sind und dem Stand der Technik entsprechen.

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher ist die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich zu behandeln!

[8] Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de/gshb/deutsch/index.htm)

# Datenschutz bei externer Wartung und Systembetreuung

| Informationen und Unterlagen | Bemerkungen |
|---|---|
| Welche Firmen führen Wartungsarbeiten durch: | |
| Wartungsvertrag vom:<br>(ggf. als Anlage beifügen) | |
| Um welche Wartungsarbeiten handelt es sich: | |
| Um welche Art von Wartung handelt es sich:<br>• Arbeiten vor Ort<br>• Wartungsarbeiten und Systembetreuung außer Ort<br>• Fernwartung | |
| In welchem Umfang wird die Wartung durchgeführt:<br>• Gelegentlich bei Bedarf<br>• Regelmäßig<br>• Wartungspersonal ist ständig vor Ort | |

| **Klassifizierung der Schutzstufe**<br>**Begründung der Einstufung (Extrablatt)** | | | | |
|---|---|---|---|---|
| **Stufe A** | **Stufe B** | **Stufe C** | **Stufe D** | **Stufe E** |
| | | | | |

**Erläuterung**:

Die einzelnen Anforderungen sind nach dem Schutzstufenkonzept[9] gestaffelt aufgeführt. Die Grundschutzforderungen unter der Schutzstufe A – B sind immer anzuwenden. Die unter den Schutzstufen C, D oder E aufgeführten Anforderungen kommen aufgrund der höheren Datenschutzsicherungsanforderung jeweils ergänzend hinzu.

Anmerkung:
Grundsätzlich reicht eine Schutzstufenklassifizierung allein allerdings nicht aus, um daraus direkt die erforderlichen und angemessenen technisch-organisatorischen Sicherheitsmaßnahmen abzuleiten. Soll dies erreicht werden, ist das **Schadenspotential** einer Gefährdung im Rahmen einer Gefahren- und Risikoanalyse gemeinsam mit deren **Eintrittswahrscheinlichkeit** zu bewerten. Erst hieraus lassen sich bestimmte Schutzbedarfskategorien entwickeln, für die adäquate Sicherheitsmaßnahmen definiert werden können.
Im Rahmen dieser Orientierungshilfe, die vor allem der Heranführung und Problematisierung dienen soll, wird aus Gründen der Notwendigkeit generalisierender Aussagen bewusst auf ein zu komplexes und in der Darstellung unübersichtliches Bewertungsverfahren verzichtet.
Dies ist im Einzelfall - insbesondere im Rahmen einer Vorabkontrolle[10] - nachzuführen.

[9] www.lfd.niedersachsen.de >Service-Angebote >Technische Hilfen >Schutzstufen
[10] www.lfd.niedersachsen.de >Service-Angebote >Technische Hilfen >Vorabkontrolle

| 1 | Allgemeine Anforderungen | Erfüllt | Nicht erfüllt | Trifft nicht zu | Bemerkung |
|---|---|---|---|---|---|
| **Daten der Schutzstufe A + B:** | | | | | |
| **1.1** | Art und Umfang der Wartung sind schriftlich vereinbart. | | | | |
| **1.2** | Kompetenzen und Pflichten zwischen Wartungspersonal und eigenem Personal sind eindeutig festgelegt. | | | | |
| **1.3** | Das Wartungspersonal ist schriftlich auf das Datengeheimnis verpflichtet (§ 5 BDSG) bzw. darüber belehrt worden (§ 5 NDSG). | | | | |
| **1.4** | Das Wartungspersonal hat nur die Zutritts-, Zugangs und Zugriffsrechte, die für die Wartung erforderlich sind. | | | | |
| **1.5** | Soweit möglich, sind personenbezogene Daten aus dem direkten Zugriff des Wartungspersonals entfernt worden. | | | | |
| **1.6** | Weitergegebene Daten sind ausschließlich zum Zwecke der Wartung zu verwenden. | | | | |
| **1.7** | Die Weitergabe von Daten durch das Wartungspersonal an Dritte ist untersagt. | | | | |
| **1.8** | Weitergegebene Daten werden nach Abschluss der Wartungsarbeiten zurückgegeben oder unverzüglich gelöscht. | | | | |
| **1.9** | Der Auftraggeber überprüft regelmäßig die Einhaltung der vereinbarten Sicherheitsmaßnahmen. | | | | |
| **1.10** | In allen Phasen der Wartungsarbeiten werden angemessene Virenschutz-Maßnahmen getroffen. | | | | |
| **1.11** | Die Wartungsarbeiten können jederzeit durch den Auftraggeber abgebrochen werden. | | | | |

| 1 | noch<br>Allgemeine Anforderungen | Erfüllt | Nicht erfüllt | Trifft nicht zu | Bemerkung |
|---|---|---|---|---|---|
| **Daten der Schutzstufe C:** | | | | | |
| **1.12** | Die vom Auftragnehmer zu treffenden / einzuhaltenden Sicherungsmaßnahmen sind schriftlich vereinbart. | | | | |
| **1.13** | Für regelmäßige Wartungsarbeiten liegt ein gegenseitig abgestimmter Terminplan vor. | | | | |
| **1.14** | Art, Umfang und Zeitpunkt der durchgeführten Wartungsarbeiten werden schriftlich festgehalten (Ergebnisse, Arbeitsbeginn und -ende, Name des Wartungstechnikers) oder entsprechend revisionssicher elektronisch dokumentiert. | | | | |
| **1.15** | Die speziellen Benutzerkennungen werden nur für unmittelbare Wartungsarbeiten freigegeben, ansonsten sind sie gesperrt.<br>Die Freigabe erfolgt durch den Auftraggeber. | | | | |
| **1.16** | Die dem Wartungstechniker eingeräumten Zutritts-, Zugangs- und Zugriffsrechte sind nach Abschluss der Arbeiten widerrufen bzw. gelöscht worden. | | | | |
| **1.17** | Soweit die eigenen Administratoren nicht mehr die notwendigen Fachkenntnisse besitzen, um die Tätigkeiten des Wartungspersonals nachzuvollziehen, wird verstärkt dokumentiert und protokolliert um ggfs eine Kontrolle durch sachkundige Dritte gewährleisten zu können. | | | | |
| **Daten der Schutzstufe D:** | | | | | |
| **1.18** | Der Kreis der Zutritts-, Zugangs- und Zugriffsberechtigten ist schriftlich festgelegt. | | | | |
| **Daten der Schutzstufe E:** | | | | | |
| **1.19** | Die Zuverlässigkeit des Wartungspersonals wird vom Auftraggeber überprüft<br>(z.B. Führungszeugnis). | | | | |
| **1.20** | Ggf. Zusatzfrage/-anforderung: | | | | |

| 2 | Wartung und Systembetreuung vor Ort | Erfüllt | Nicht erfüllt | Trifft nicht zu | Bemerkung |
|---|---|---|---|---|---|
| **Daten der Schutzstufe A + B:** | | | | | |
| **2.1** | Die Wartungstechniker weisen sich vor Beginn der Arbeiten aus. | | | | |
| **Daten der Schutzstufe C:** | | | | | |
| **2.2** | Regelungen über die Beaufsichtigung des Wartungspersonals liegen vor. | | | | |
| **Daten der Schutzstufe D:** | | | | | |
| **2.3** | Eine fachkundige Kraft beaufsichtigt die Arbeiten. | | | | |
| **2.4** | Ggf. Zusatzfrage/-anforderung: | | | | |

| 3 | Externe Wartung und Systembetreuung außer Haus | Erfüllt | Nicht erfüllt | Trifft nicht zu | Bemerkung |
|---|---|---|---|---|---|
| **Daten der Schutzstufe A + B:** | | | | | |
| **3.1** | Alle personenbezogenen Daten werden vor Beginn der Wartung gelöscht.<br>Ausnahmen sind schriftlich begründet. | | | | |
| **3.2** | Es werden Nachweise über den Versand geführt (Begleitzettel, Versandscheine, Empfangsbestätigung). | | | | |
| **3.3** | Bei Rückgabe der Geräte wird die Vollständigkeit geprüft und dokumentiert. | | | | |
| **3.4** | Alle Passwörter der DV-Anlage oder Softwareprodukte werden nach Rückgabe der Geräte geändert. | | | | |
| **Daten der Schutzstufe C:** | | | | | |
| **3.5** | Bei Versand werden verschlossene Behältnisse verwendet. | | | | |
| **Daten der Schutzstufe D:** | | | | | |
| **3.6** | Der Transportweg und die am Transport beteiligten Personen sind schriftlich festgelegt. | | | | |
| **3.7** | Alle Dateien oder Softwareprodukte sind nach Rückgabe auf Integrität geprüft. | | | | |
| **3.8** | Ggf. Zusatzfrage/-anforderung: | | | | |

| 4 | Fernwartung | Erfüllt | Nicht erfüllt | Trifft nicht zu | Bemerkung |
|---|---|---|---|---|---|
| **Daten der Schutzstufe A + B:** | | | | | |
| **4.1** | Für alle Fernwartungsmöglichkeiten besteht ein regelmäßig überprüftes Datensicherungskonzept. | | | | |
| **4.2** | Alle Fernwartungsaktivitäten werden protokolliert. Die Protokollinhalte sind dem ändernden Zugriff | | | | |
| **4.3** | Der Dialog mit der Fernwartungszentrale wird beendet, wenn die Wartungsarbeiten abgeschlossen sind oder die Verbindung zur Fernwartungszentrale gestört ist („Zwangslogout"). | | | | |
| **4.4** | Dateien oder Programme werden von der Fernwartungsstelle nur nach vorheriger Absprache angelegt. | | | | |
| **Daten der Schutzstufe C + D:** | | | | | |
| **4.5** | Die Verbindung oder Freischaltung wird vom Auftraggeber aus aufgebaut (Call-Back-Verfahren) und überwacht. | | | | |
| **4.6** | Die Übertragung personenbezogener Daten auf leitungsgebundenen oder drahtlosen Übertragungswegen ist durch ein nach dem Stand der Technik hinreichend sicheres kryptographisches Verfahren gesichert. | | | | |
| **4.7** | Fernwartungspasswörter werden nur verschlüsselt übertragen (möglichst Challenge-Response-Verfahren). | | | | |
| **4.8** | Der Ort, von wo aus die Fernwartung durchgeführt wird, ist schriftlich festgelegt. | | | | |
| **Daten der Schutzstufe E:** | | | | | |
| **4.9** | Bei Verarbeitung von personenbezogenen Daten der Schutzstufe E wird keine Fernwartung durchgeführt. | | | | |
| **4.10** | Ggf. Zusatzfrage/-anforderung: | | | | |