

Herzlich Willkommen



Datenschutz bei Fernzugriff; Risiken und Lösung



von

Stefan Herold, Partner der
Aarcon Unternehmensberatung
Prinzregentenstraße 124

Im Prinzregentenhof


D-81677 München

Telefon: +49 89 244 10 55-0

stefan.herold@aarcon.net

www.aarcon.net

**Euro-Assessor EFQM, Qualitäts-, Umwelt und Datenschutzbeauftragter
Beratung zu integrierten Managementsystemen nach ISO 9001, 14001, 18001,
DIN EN 50518, DIN 77200, CE-Konformität, Anerkennungsverfahren (VdS),
OHSAS, SCC**

- Intention zur Fernparametrierung
- Risiken und Regelungen 
- Präventionsmaßnahmen
- Sanktionen bei Verstößen gegen den Datenschutz
- Datenschutz
 - § 11 BDSG, Erhebung, Verarbeitung, Nutzung von Daten
 - § 9 BDSG, Technische und organisatorische Maßnahmen
- Mustergliederung einer Vereinbarung zum Datenschutz bei Fernparametrierung
- Hilfestellungen



= KOSTENSENKUNG

Instandhaltung

Wartung (Erhalt des Sollzustandes)



Inspektion (Feststellung und Beurteilung des Istzustandes)

Instandsetzung (Herstellung der Funktionsfähigkeit)

Verbesserung (Steigerung der Funktionssicherheit)

Weitere Intention

Abruf von Ereignissen

Abruf von Daten



Änderung von Einstellungen (Parametern)



.....

Verlust der ordnungsgemäßen Funktionsfähigkeit der Anlage

durch z.B. Abschaltung von Meldergruppen

Veränderung der Auslösekriterien bzw.
ungeschützter Abruf von Daten



Datenmissbrauch

Regelungen dazu:

Europäische Datenschutzverordnung (1/2012) im Entwurf

RiLi 95/46 EG Datenschutzrichtlinie

Bundesdatenschutzgesetz BDSG

Telekommunikationsgesetz TKG und Telemediengesetz TMG

VDE 0833, Forderungen an Übertragung

VdS – Richtlinie E VdS 3169 „Fernzugriff.....“

BHE – Information 4 / 2000



Gegen Datenmissbrauch

Prävention



Einhaltung gesetzlicher Maßgaben

Grundsätzlich erlaubt, jedoch besondere Sorgfalt, wenn auf personenbezogene Daten zugegriffen werden kann (Name, Alter, Beruf, Post- und E-Mail-Anschrift oder Hobbys...)

Diese Daten unterliegen den Anforderungen des Bundesdatenschutzgesetzes BDSG, des Telemediengesetzes TMG und des Telekommunikationsgesetzes TKG.

Eine Fernwartung entspricht einer Auftragsdatenverarbeitung gem. § 11 BDSG auch dann, wenn der Kunde seinen Sitz innerhalb der EU hat (Harmonisierung des Datenschutzrechts, RiLi 95/46 EG Datenschutzrichtlinie)

Derzeit in der Entstehung: Europäische Datenschutzverordnung (E)

Vorschlag des Europäischen Parlaments und des Rates

“zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“ vom 25.01.2012

- **§ 43 II BDSG (Bußgeldvorschrift)**



Ordnungswidrigkeit, d.h. Strafe: Bußgeld teilw. bis zu € 50.000,--)



- **§ 44 BDSG (Strafvorschrift)**



**Straftatbestand, d.h. Freiheitsstrafe bis 2 Jahren
oder Geldstrafe (Antragsdelikt)**



- **§ 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses)**



**Straftatbestand, d.h. Freiheitsstrafe bis 5 Jahren
oder Geldstrafe (Offizialdelikt)**



- **§ 17 UWG (Verrat von Geschäfts- und Betriebsgeheimnissen)**



**Straftatbestand, d.h. Freiheitsstrafe bis 3 Jahren
oder Geldstrafe (Antragsdelikt)**



Fernwartung durch Dritte erfordert auf jeden Fall eine schriftliche Regelung !

§ 11 BDSG / II: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Der **Auftrag** ist **schriftlich** zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:



- ✓ 1. der **Gegenstand** und die **Dauer des Auftrags**,
- ✓ 2. der **Umfang, die Art und der Zweck** der vorgesehenen Erhebung, Verarbeitung oder **Nutzung** von Daten, die Art der Daten und der Kreis der Betroffenen,
- ✓ 4. die **Berichtigung, Löschung und Sperrung von Daten**,
- ✓ 5. die nach **Absatz 4 bestehenden Pflichten des Auftragnehmers**, insbesondere die von ihm vorzunehmenden **Kontrollen**, 
- ✓ 6. die etwaige **Berechtigung zur Begründung von Unterauftragsverhältnissen**, 

Fernwartung durch Dritte erfordert auf jeden Fall eine schriftliche Regelung !

§ 11 BDSG / II: Seite 2



- ✔ 7. **die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,**
- ✔ 8. **mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,**
- ✔ 9. **der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,**
- ✔ 10. **die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.**



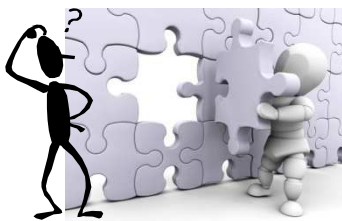
Empfehlung zur Fernwartung:

§ 9 BDSG: Technische und organisatorische Maßnahmen



Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten.

Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.



Empfehlung zur Fernwartung:

§ 9 BDSG: Technische und organisatorische Maßnahmen










- wie z.B.
 - **Wirksame Absicherung der datenverarbeitenden Einrichtungen gegen unbefugten Zugang und**
 - **Definition im Datensicherheitskonzept**
 - **Zugänglichkeit des DS-Konzeptes für den Kunden**
 - **Anhang zur Fernwartungsvereinbarung**
 - **Kontrollrecht des Kunden oder eines von ihm beauftragten Dritten**
 - (z.B. Auditor für Datenschutz)...










Präambel / Ziel der Vereinbarung



- § 1 Gegenstand und Dauer des Auftrags zu § 11/II Nr. 1 BDSG 
- § 2 Umfang der Auftragsdatenvereinbarung zu § 11/II Nr. 2 BDSG 
- § 3 Technische und organisatorische Maßnahmen zum Datenschutz zu § 11/II Nr. 3 BDSG 
- § 4 Berichtigung, Löschung und Sperrung von Daten zu § 11/II Nr. 4 BDSG 
- § 5 Pflichten des Auftragnehmers zu § 11/II Nr. 5 BDSG 
- § 6 Begründung von Unterauftragsverhältnissen zu § 11/II Nr. 6 BDSG 
- § 7 Kontrollen zu § 11/II Nr. 7 BDSG 

Präambel / Ziel der Vereinbarung



§ 8 Verstöße gegen Vorgaben zum Datenschutz	zu § 11/II Nr. 8 BDSG	
§ 9 Weisungsbefugnisse	zu § 11/II Nr. 9 BDSG	
§ 10 Verfahren bei Auftragsbeendigung	zu § 11/II Nr. 10 BDSG	
§ 11 Maßnahmen Dritter oder Rechte Dritter	zu § 11/II Nr. 7 BDSG	
§ 12 Zurückbehaltungsrecht	zu § 11/II Nr. 10 BDSG	
§ 13 Ort der Auftragsdatenverarbeitung	zu § 9 BDSG	
§ 14 Zugehörige Unterlagen / Anlagen	zu § 9 BDSG	
§ 15 Schlussbestimmungen	-	

Weitere Hilfe z. B. über BHE:

Info zu Fernparametrierung bei Gefahrenmeldeanlagen 04/2000



Technische Maßnahmen als Empfehlung daraus:



- Modem im gesicherten Bereich der GMA als Bestandteil dessen
- Sabotagefreischaltung bei kombinierten Modemgeräten
- Anruf zum Zwecke der Daten- bzw. Parameterabfrage von Berechtigten zu jeder Zeit

Schutzmechanismen gegen unberechtigte Abfrage:

- Modem reagiert nur auf berechtigte Anschlüsse bei Rufnummernübermittlung
- Passwortidentifizierung und ggf. weitere Identifizierung erforderlich
- ohne Rufnummernübermittlung: erfolgt RR nach Identifikation des Anschlusses



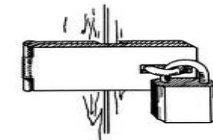
Weitere Hilfe z. B. über BHE:

Info zu Fernparametrierung bei Gefahrenmeldeanlagen 04/2000



weitere Schutzmaßnahmen bei Veränderung von Einstellungen, Parametern und Daten, z.B. willentliche, einmalige und zeitbegrenzte Freigabe durch Anlagenbetreiber

(Codeeingabe, Schlüsselschalter, Dongle, Kopierschutz...)



- Softwareschutz vor unberechtigtem Betrieb der eigenen Fernwirksoftware
- Dokumentation des Fernzugriffes im anlageeigenen Ereignisspeicher

Organisatorische Maßnahmen:



- Freigabe des Fernzugriffes nur durch autorisierte Personen des Betreibers
- Zugriff durch externe nur durch vorher benannte Personen mit Codewort

***Vielen Dank für Ihre
Aufmerksamkeit***