Best Practices: „Fernwartung in der Gesundheitsversorgung“

Eine Ausarbeitung von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe Datenschutz & IT-Sicherheit

Historie

Version 1

Stand der Bearbeitung: 17. August 2021

An der Ausarbeitung beteiligte Personen (Nennung in alphabetischer Reihenfolge):

Berger, Chris	Doctolib GmbH
Dörr, Michael	ARZsoftware eG
Geisthardt, Dennis	Bundesverband Gesundheits-IT – bvitg e. V.
Isele, Christoph	Cerner Deutschland GmbH
Kremers, Marcus	VISUS Health IT GmbH
Liebscher; Thomas	Philips GmbH
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

- Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
- Im folgenden Text wird, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
- Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

D. h. Sie dürfen:

Teilen: das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten und zwar für beliebige Zwecke, sogar kommerziell.

Der Lizenzgeber kann diese Freiheiten nicht widerrufen solange Sie sich an die Lizenzbedingungen halten.

Unter folgenden Bedingungen:

Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.

Keine Bearbeitungen: Wenn Sie das Material remixen, verändern oder darauf anderweitig direkt aufbauen, dürfen Sie die bearbeitete Fassung des Materials nicht verbreiten.

Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

https://creativecommons.org/licenses/by-nd/4.0/deed.de

bzw. für den vollständigen Lizenztext

https://creativecommons.org/licenses/by-nd/4.0/legalcode.de

Inhaltsverzeichnis

1 Einführung in das Thema

Nicht bei jedem Fernwartungsvorgang müssen Patientendaten verarbeitet werden, beispielsweise ist im Rahmen des Einspielens von Sicherheitsupdates zum genutzten Betriebssystem i. d. R. ein Zugriff auf Patientendaten nicht erforderlich und darf deshalb auch nicht erfolgen.

Bei der Wartung der Anwendungsapplikation ist der Zugriff auf Patientendaten im Rahmen von Unterstützungsleistungen die Regel. Beispielsweise können Unstimmigkeiten in den Abrechnungsdaten bei einem konkreten Fall nur mit Überprüfung der in diesem Fall vorliegenden konkreten Daten beseitigt werden, die Beseitigung von Ungereimtheiten bei der Weitergabe von Patientendaten z. B. im Rahmen der gesetzlichen Qualitätssicherung oder einer Krebsregistermeldung erfordern den Zugriff auf die betroffenen Patientendaten. Natürlich muss im Rahmen der hier beschriebenen Fernwartungsvorgänge ein entsprechendes Schutzniveau der betroffenen Daten gewährleistet werden.

Die Anforderungen zum Schutz personenbezogener Daten in der DS-GVO sind allgemeiner Natur und sind nicht spezifisch genug, dass sie eine direkte Umsetzung ermöglichen. D. h., es ist ein hoher Grad an Interpretation vorhanden, was ein „angemessenes Schutzniveau“ darstellt.

Andererseits erfordert eine über das Internet oder andere Kommunikationsnetze erfolgende Fernwartung immer eine Öffnung des eigenen Netzes nach außen, d. h. letztlich muss eine Lücke in den Schutzmaßnahmen geöffnet werden. Eine derartige Lücke bietet potenziell eine zusätzliche Angriffsfläche, so dass eine Fernwartung entsprechende Schutzmaßnahmen erfordert. Ergänzend gehören Gesundheitsdaten zu den Daten mit dem höchsten Schutzniveau, so dass nachvollziehbarere Regelungen zur Gewährleistung des angemessenen Schutzniveaus erforderlich sind.

Diese Best Practices beschreiben, wie der Schutz personenbezogener Daten gegen unrechtmäßige Verarbeitung im Rahmen der Fernwartung sowohl für den ambulanten als auch stationären Sektor gesichert werden sollten. Dabei bezieht sich die Ausarbeitung sowohl auf Patientendaten als auch auf Beschäftigtendaten. Unter Fernwartung werden im Folgenden Tätigkeiten zur Inspektion, Wartung, Pflege und Fehlerbehebung der in diesen Sektoren eingesetzten IT-Systeme verstanden. Diese Tätigkeiten finden in der Regel über eine Rechnerverbindung (Internet) statt.

2 Rechtliche Rahmenbedingungen

Diese Best Practices adressieren die Sicherheit der Verarbeitung, daneben müssen selbstverständlich auch Regelungen zu anderen Tatbeständen wie beispielsweise Erlaubnistatbeständen oder dem Vorhandensein eines ggf. benötigten Vertrages zur Auftragsverarbeitung Bestandteil dieser Best Practices sein, da die Sicherheit grundsätzlich nur im Rahmen einer rechtlich erlaubten Verarbeitung gewährleistet sein kann: eine gesetzeswidrige Verarbeitung stellt per definitionem schon eine unsichere Verarbeitung dar. Daher muss neben den reinen technischen Anforderungen zur Sicherheit der Verarbeitung auch die entsprechenden organisatorischen Erfordernisse abgebildet werden.

2.1 Datenschutz-Grundverordnung (DS-GVO)

Im Rahmen der Fernwartung im hier beschriebenen Kontext können sowohl Patienten- wie auch Beschäftigtendaten verarbeitet werden, so dass insbesondere der Geltungsbereich der DS-GVO gegeben ist. Die DS-GVO enthält für diese Datenkategorien diverse Öffnungsklauseln für den nationalen Gesetzgeber, so dass neben dem europäischen auch das deutsche Recht betrachtet werden muss.

Die Verarbeitung der personenbezogenen Daten muss erlaubt sein, wobei im Rahmen der Verarbeitung von Beschäftigtendaten je nach verarbeiteten Datenkategorie Art. 6 DS-GVO oder auch Art. 9 DS-GVO zu beachten ist, im Rahmen der Verarbeitung von Patientendaten ist immer Art. 9 DS-GVO Voraussetzung für eine erlaubte Verarbeitung, ggf. jeweils in Kombination mit dem Recht des Mitgliedstaates. Dabei stellt die Fernwartung jedoch nur eine Besonderheit bzgl. des Ortes der Verarbeitung dar, nicht jedoch der Verarbeitung an sich. D. h. für die Tatsache, dass eine Fernwartung durchgeführt wird, ist kein separater Erlaubnistatbestand erforderlich; abgesehen von einer Verarbeitung in einem Drittland, was nur entsprechend den Vorgaben von Kapitel V DS-GVO statthaft ist.

Werden externe Kräfte mit der Fernwartung beauftragt, wird dies regelhaft eine Verarbeitung im Auftrag darstellen, so dass insbesondere ein Vertrag entsprechend Art. 28 DS-GVO erforderlich ist.

Insbesondere die Artt. 25, 32 und 35 DS-GVO enthalten Anforderungen hinsichtlich der Sicherheit der Verarbeitung und müssen dementsprechend berücksichtigt werden.

2.2 Deutsches Recht

Die Regelungen bzgl. der Verarbeitung von Gesundheitsdaten sind auf Grund der konkurrierenden Gesetzgebung sowohl im Bundes- als auch im Landesrecht vorhanden, so dass verschiedene rechtliche Rahmenbedingungen zu prüfen sind.

Grundsätzlich ist die Rechtmäßigkeit der Verarbeitung unabhängig von der Tatsache, ob die Verarbeitung vor Ort oder an einem anderen Ort erfolgt, gegeben: Entweder ist der Verarbeitung inkl. der Fern-Verarbeitung erlaubt oder nicht.

Speziell bei der Verarbeitung durch externe Kräfte bestehen jedoch spezialgesetzliche Voraussetzungen:

- § 203 StGB „Verletzung von Privatgeheimnissen“
  § 203 StGB enthält die Vorgaben hinsichtlich der Verarbeitung von Privatgeheimnissen von Berufsgeheimnisträgern, was insbesondere auch die Patientendaten die von Ärzten, Zahnärzten, Tierärzten, Apothekern oder Angehörigen eines anderen Heilberufs, der für die

Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, verarbeitet werden.

Grundsätzlich ist die Verarbeitung durch externe Kräfte erlaubt, aber nur unter den Voraussetzungen von § 203 Abs. 3,4 StGB.

- Berufsrecht

  Ärzte, Zahnärzte, Apotheker und Psychotherapeuten unterliegen Berufsordnungen, die von den jeweils für den Beruf zuständigen Kammer mit Zustimmung der zuständigen Aufsichtsbehörde (d.i. i.d.R. das jeweilige Gesundheitsministerium des Bundeslandes) verabschiedet werden.

  - Berufsordnung für Ärzte

    In jedem Bundesland existiert eine Landesordnung für die in diesem Bundesland arbeitenden Ärztinnen und Ärzte, welche wiederum auf der von der Bundesärztekammer herausgegebene Muster-Berufsordnung der Ärzte(MBO-Ä) beruhen. § 9 Abs. 3 MBO-Ä enthält Offenbarungsbefugnisse gegenüber Mitarbeiterinnen und Mit-arbeitern sowie Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, § 9 Abs. 4 MBO-Ä Mitarbeiterinnen und Mitarbeitern von Dienstleistungsunternehmen sowie sonstigen Personen, die an der beruflichen Tätigkeit mitwirken.

    D. h. Ärztinnen und Ärzten ist der Einsatz externer Kräfte grundsätzlich gestattet.
  - Berufsordnung für Zahnärzte

    Analog zu den Regelungen der Ärzte gibt die Bundeszahnärztekamme eine Musterberufsordnung heraus. § 7 Abs. 3 enthält eine Offenbarungsbefugnis gegenüber Praxismitarbeitern sowie sonstigen Personen, die an der beruflichen Tätigkeit mitwirken.
  - Berufsordnung der Apothekerkammer

    Die Landesapothekerkammern geben die jeweilige Landesberufsordnung heraus. Jede der Landesberufsordnungen enthält einen Abschnitt, der Regelungen zur Verschwiegenheit beinhaltet und insbesondere auf die Einhaltung von § 203 StGB verweist, ansonsten nur durch gesetzliche Regelungen erlaubte Verarbeitung gestattet. Damit ist insbesondere eine Verarbeitung im Auftrag zur erforderlichen Wartung der in der Apotheke eingesetzten IT-Systeme statthaft.
  - Berufsordnung für Psychotherapeuten

    Die Muster-Berufsordnung der Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten enthält in § 8 Abs. 5 eine Offenbarungsbefugnis gegenüber den berufsmäßig tätigen Gehilfinnen und Gehilfen und den zur Vorbereitung auf den Beruf tätigen Personen sowie den sonstigen Personen, die an der beruflichen oder dienstlichen Tätigkeit der Psychotherapeutinnen und Psychotherapeuten mitwirken.

- Krankenhäuser
  - In Deutschland wird die Verarbeitung von Patientendaten in Krankenhäuser, welche der Landesförderung unterliegen, in Landesgesetzen geregelt. Outsourcing bzw. Auftragsverarbeitung ist in den landesrechtlichen Regelungen grundsätzlich gestattet, jedoch wird in einigen Landesgesetzen der Ort der Verarbeitung eingeschränkt, was entgegen den Bestimmungen von Art. 1 Abs. 3 DS-GVO erfolgt.
  - Krankenhäuser, die nicht der Landesförderung unterliegen, unterliegen wiederum der jeweiligen eigenen Gesetzgebung:

- Krankenhäuser des Bundes wie Bundeswehrkrankenhäuser: Gesetzgebung Bund.
- Krankenhäuser der Kirche: Gesetzgebung der evangelischen bzw. katholischen Kirche. Nahezu alle kirchlichen Krankenhäuser unterliegen jedoch der Landesförderung, so dass auch für diese kirchlichen Krankenhäuser die jeweiligen Landeskrankenhausbestimmungen (inkl. der datenschutzrechtlichen Regelungen) gelten. Dies führt häufig dazu, dass bzgl. Personaldaten kirchliches Datenschutzrecht gilt, für Patientendaten das jeweilige Landesrecht.

  Sowohl im evangelischen wie auch im katholischen Recht wurden die datenschutzrechtlichen Vorgaben der DS-GVO angepasst, eine Verarbeitung im Auftrag ist grundsätzlich auch für nicht zur Kirche gehörenden Auftragnehmer gestattet.
- Auch die meisten privatwirtschaftlich geführten Krankenhäuser werden vom jeweiligen Land gefördert und hier gilt bzgl. der Patientendaten dann i.d.R. ebenfalls das jeweilige Landeskrankenhausgesetz, bzgl. der Personaldaten i.d.R. jedoch das entsprechende Bundesrecht.

  Es gibt jedoch auch einige Privatkliniken in Deutschland, die nur Privatpatienten behandeln und auf jegliche Landesförderung verzichten. Für diese gilt dann nur das jeweilige Bundesrecht.

– Sozialdatenschutz

  Die Definition von Sozialdaten findet sich in § 67 Abs. 2 SGB X: Sozialdaten sind personenbezogene Daten, die von einer in § 35 SGB I genannten Stelle, dies sind
  - die Verbände der Leistungsträger,
  - die Arbeitsgemeinschaften der Leistungsträger
  - die Verbände der Leistungsträger,
  - die Datenstelle der Rentenversicherung,
  - die in diesem Gesetzbuch genannten öffentlich-rechtlichen Vereinigungen,
  - Integrationsfachdienste,
  - die Künstlersozialkasse,
  - die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist,
  - die Behörden der Zollverwaltung, soweit sie Aufgaben nach § 2 des Schwarzarbeitsbekämpfungsgesetzes und § 66 des Zehnten Buches durchführen,
  - die Versicherungsämter und Gemeindebehörden
  - die anerkannten Adoptionsvermittlungsstellen (§ 2 Abs. 2 AdVermiG), soweit sie Aufgaben nach diesem Gesetzbuch wahrnehmen,
  - die Stellen, die Aufgaben nach § 67c Abs. 3 SGB X, d. h.
    - Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen,
    - Rechnungsprüfung,
    - Durchführung von Organisationsuntersuchungen,
    - Verarbeitung zu Ausbildungs- und Prüfungszwecken,

    wahrnehmen,

  im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.

Für all diese Stellen gilt bzgl. Verarbeitung im Auftrag die Vorgaben von § 80 SGB X, d. h. die Verarbeitung im Auftrag ist grundsätzlich erlaubt. Jedoch werden die Möglichkeiten zur Verarbeitung in einem Drittstaat auf Art. 45 DS-GVO eingeschränkt.

3 Anforderungen bzgl. der sicheren Gestaltung von Fernwartungsvorgängen

3.1 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

In den Vertraulichkeits- oder Geheimhaltungsvereinbarungen müssen unter Verwendung rechtsverbindlicher Begriffe die Rahmenbedingungen und Anforderungen zum Schutz vertraulicher Informationen beschrieben werden. Dazu gehören insbesondere

3.1.1 Definition der zu schützenden Informationen

Der Verantwortliche muss die zu schützenden Informationen/Daten benennen. Hinweise auf Hilfestellungen finden sich in Anhang 1.

Anforderung 1. Der Verantwortliche legt im Rahmen der Fernwartung für die betroffenen Anwendungen, IT-Systeme und Kommunikationsverbindungen den Schutzbedarf der potentiell zu verarbeitenden Daten fest.

3.1.2 Vertragsdauer

Die Dauer der vertraglichen Beziehungen muss geregelt werden. Dies kann entweder durch die Angabe eines bestimmten Datums für Beginn und Ende sein, das Ende der Vertragsbeziehung kann aber auch durch nachvollziehbare Kriterien (z. B. „endet zeitgleich mit der Nutzung des Systems xy, für welches die Fernwartung beauftragt wird“) festgelegt werden.

Anforderung 2. Die Dauer des Vertragsverhältnisses zur Fernwartung muss vereinbart werden.

3.1.3 Verarbeitung personenbezogener Daten durch den Fernwartenden

Art. 28 Abs. 3 lit. b schreibt vor, dass mit „zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet werden“. Jedoch existieren darüber hinaus auch noch Personen, die auf Grund ihrer Tätigkeit evtl. Zugriffsmöglichkeiten haben, wenngleich diese Personen nicht zur Verarbeitung befugt sind. Der Auftragsverarbeiter muss daher gewährleisten, dass alle von ihm eingesetzten Personen auf die Wahrung der datenschutzrechtlichen Pflichten insbesondere auf die Geheimhaltung bzgl. personenbezogener Daten verpflichtet bzw. unterwiesen wurden, nicht nur die mit der vorliegenden konkreten Verarbeitungstätigkeit befugten Personen.

Anforderung 3. Alle vom Auftragsverarbeiter eingesetzten Personen, die auftragsgemäß auf personenbezogene Daten des Verantwortlichen zugreifen können, werden von ihm auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt.

Im Rahmen der Fernwartung kann ggf. auch das Fernmeldegeheimnis berührt werden, sodass eine Verpflichtung der Beschäftigten nach § 88 TKG erforderlich sein kann, auch wenn weder der Verantwortliche noch Auftragsverarbeiter ein Dienstanbieter entsprechend der Definition von § 7 Ziff. 6 TKG ist. Dies kann nur im Einzelfall geprüft werden.

Anforderung 4. Die Wahrung des Fernmeldegeheimnisses entsprechend §88 TKG muss von Verantwortlichem und Auftragsverarbeiter gewährleistet werden. Dazu müssen Verantwortlicher und Auftragsverarbeiter alle Personen, die auftragsgemäß auf personenbezogene Daten mittels Verfahren der Telekommunikation wie Telefon oder E-Mail zugreifen können, auf das Fernmeldegeheimnis verpflichten und über die sich daraus ergebenden besonderen Geheimhaltungspflichten belehren.

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) definiert in § 2 Ziffer 1 den Begriff des „Geschäftsgeheimnisses“ und verbietet in § 4 den Verrat von Geschäftsgeheimnissen. Insbesondere verbietet § 4 Abs. 2 Ziff. 3 GeschGehG ein Geschäftsgeheimnis zu nutzen oder offenzulegen, wenn eine Verpflichtung existiert, nach welcher Geschäftsgeheimnisse geheim zu halten sind. Neben den üblichen Geschäfts- und Betriebsgeheimnissen sind auch die während der Tätigkeit für den Verantwortlichen vom Auftragsverarbeiter erlangten Patientendaten als derartige Geheimnisse zu werten, deren Weitergabe strafrechtlich verfolgt werden kann.

Anforderung 5. Alle vom Verantwortlichen und vom Auftragsverarbeiter im Rahmen des Auftrags eingesetzten Personen müssen bzgl. der Pflichten zur Wahrung von Geschäfts- und Betriebsgeheimnissen des Verantwortlichen bzw. des Auftragsverarbeiters hingewiesen werden.

Im Gesundheitswesen werden oftmals personenbezogene Daten verarbeitet, die unter die Regelungen des § 203 StGB fallen. Erfolgt hier eine Verarbeitung durch Dienstleister, ist eine Verpflichtung gemäß den Vorgaben von § 203 Abs. 4 StGB erfolgen. Ein Muster zur vertraglichen Gestaltung wie auch zu einer Verpflichtungserklärung wurde einigen Verbänden erarbeitet und steht im Internet frei zum Download zur Verfügung[1]. Ob eine entsprechende Verpflichtung erforderlich ist, kann nur im Einzelfall entschieden werden.

Anforderung 6. Der Auftragsverarbeiter setzt nur Personen ein, die auf die Einhaltung der Vorgaben von § 203 StGB verpflichtet wurden, wenn von § 203 StGB geschützte Daten zu den im Rahmen der vertraglichen Vereinbarung verarbeitenden Daten gehören, insbesondere auch die Geheimhaltungspflichten bzgl. Berufsgeheimnissen sowie Betriebs- und Geschäftsgeheimnissen.

In komplexen Vertragssituationen kann die Notwendigkeit für den Einsatz von Unterauftragnehmern entstehen. Der Auftragsverbeiter stellt sicher, dass Unterauftragnehmer in Bezug auf die Verarbeitung personenbezogener Daten an dieselben vertraglichen Pflichten gebunden sind wie der Auftragsverarbeiter selbst gemäß der Vereinbarung mit dem Verantwortlichen. Dabei muss dem jeweiligen Unterauftragnehmer natürlich nur die Pflichten auferlegt werden, die seinen Teil der Verarbeitung der personenbezogenen Daten betreffen.

Anforderung 7. Der Auftragsverarbeiter gewährleistet, dass Unterauftragnehmer bzgl. der durch sie erfolgenden Verarbeitung personenbezogener Daten an dieselben vertraglichen Pflichten gebunden werden.

3.1.4 Rechte des Verantwortlichen

Der Verantwortliche hat das Recht, die Umsetzung der vereinbarten Regelungen zu überprüfen und zu überwachen. Eine Hilfestellung findet der Auftraggeber in Anhang 1.

Anforderung 8. Der Auftragsverarbeiter bietet dem Verantwortlichen auf dessen begründeten Wunsch hin die Möglichkeit, in regelmäßigen Abständen aber nicht häufiger als einmal im

[1] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitkom): T-Einsatz durch Berufsgeheimnisträger – Muster zur Umsetzung der Neuregelung des § 203 StGB. . [Online, zitiert am 2021-08-30]; Verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Muster-zur-Umsetzung-des-Gesetzes-zur-Neuregelung-des-Schutzes-von-Geheimnissen-bei-der-Mitwirkung-Dritter-an-der-Berufsausuebung-schweigepflichtiger-Personen.html bzw. direkt Download der pdf-Datei unter https://www.bitkom.org/sites/default/files/file/import/20180718-Muster-203StGB-final.pdf

Jahr und nur während der regulären Geschäftszeiten des Auftragsverarbeiters, einem qualifizierten, unabhängigen, vom Auftragsverarbeiter bestimmten und bezahlten externen Gutachter zu Prüfzwecken Zugang zu den Einrichtungen, die der Auftragsverarbeiter für die Verarbeitung personenbezogener Daten verwendet, zu gewähren. Dieser Gutachter muss vorab eine für den Auftragsverarbeiter angemessene Geheimhaltungsvereinbarung unterzeichnen. Alternativ bietet der Auftragsverarbeiter dem Verantwortlichen an, ein von einem qualifizierten, unabhängigen, externen Gutachter ausgestelltes Zertifikat vorzulegen, in dem bescheinigt wird, dass die Fernwartung des Auftragsverarbeiters, inklusive der eventuellen Verarbeitung personenbezogener Daten, im Einklang mit den Vereinbarungen stehen.

Anforderung 9. Der Verantwortliche verpflichtet sich,

- **a) Prüfungsanfragen mindestens 6 Wochen vor einem geplanten Prüf-Termin beim Auftragsverarbeiter schriftlich einzureichen,**
- **b) einen detaillierten und vom Auftragsverarbeiter geprüften und gebilligten Prüf-Plan vorzulegen,**
- **c) die hausinternen Vorschriften des Auftragsverarbeiters einschließlich der am Standort geltenden Gesundheits-, Sicherheits- und Geheimhaltungsbestimmungen einzuhalten und**
- **d) zur Einhaltung des geltenden Datenschutzrechts.**

Anforderung 10. Der Auftragsverarbeiter verpflichtet sich, sobald dies im Anschluss an eine Prüfung nach vernünftigem Ermessen möglich ist, dem Verantwortlichen eine Kopie des Prüfberichts zur Verfügung zu stellen. Der Verantwortliche verpflichtet sich, die erhaltenen Prüfberichte als vertrauliche Information zu behandeln.

3.1.5 Rechte des Auftragsverarbeiters

Der Auftragsverarbeiter ist innerhalb der vertraglich vereinbarten Rahmenbedingungen frei in seinen Entscheidungen. Insbesondere kann der Auftragsverarbeiter entscheiden, welches Personal er für welche Aufgaben einsetzt, sofern die Qualifikationen des eingesetzten Personals den Anforderungen der Aufgaben genügen.

Weiterhin ist der Auftragsverarbeiter nicht verpflichtet, Personaldaten an den Verantwortlichen zu übergeben, sofern nicht gesetzliche Verpflichtungen dies verlangen oder Nachweispflichten durch einen Vorfall oder eine Auskunftsanfrage eines Betroffenen dies erforderlich machen.

Anforderung 11. Der Auftragsverarbeiter ist bei der Entscheidung des eingesetzten Personals unabhängig. Er muss nur gewährleisten, dass das eingesetzte Personal die erforderliche Qualifikation zur Bearbeitung der gestellten Aufgaben hat und kann dies durch entsprechende Unterlagen wie z.B. Ausbildungs- oder Fortbildungsnachweise belegen.

3.1.6 Informationsfluss und Meldewege bei Datenpannen sowie vertragliche Regelungen bzgl. unbefugter Offenbarung

Der Verantwortliche muss den Informationsfluss und die Meldewege im Rahmen der Informationssicherheitsprozesse mit dem Auftragsverarbeiter definieren. Eine Hilfestellung siehe Anhang 1.

Anforderung 12. Der Informationsfluss und die Meldewege bei Datensicherheitsverletzungen müssen vertraglich vereinbart werden.

Anforderung 13. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Datensicherheitsverletzung unverzüglich nach Bekanntwerden. Dies gilt nicht, wenn dem eine anderslautende vollstreckungs- oder aufsichtsbehördliche Anweisung entgegensteht. In letzterem Fall wird die Meldung gemäß Anweisung der Vollstreckungs- oder Aufsichtsbehörde auf einen späteren Zeitpunkt verschoben. Art, Datum und Uhrzeit der vollstreckungs- oder aufsichtsbehördlichen Anweisung wird seitens Auftragsverarbeiter notiert und dem Verantwortlichen so bald wie möglich und zulässig zur Verfügung gestellt.

Anforderung 14. Die Meldung enthält mindestens eine grobe Beschreibung der Art der Datensicherheitsverletzung, der Kategorien und ungefähren Anzahl der betroffenen Personen, der betroffenen Unterlagen und, sofern zutreffend, der ergriffenen mildernden Maßnahmen sowie Ansprechpartner beim Auftragsverarbeiter, die den Verantwortlichen beim Umgang mit dem Vorfall unterstützen.

3.1.7 Maßnahmen bei Vertragsende

Im Wartungs- oder Leistungsvertrag oder einer entsprechenden Anlage muss geregelt werden, welche Maßnahmen am Ende des Vertrages durchgeführt werden. Gemäß Art. 28 Abs. 3 S. 2 lit. g DS-GVO müssen nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder gelöscht oder zurückgegeben werden. Jedoch bedeutet der Abschluss der Erbringung der jeweiligen Verarbeitungsleistung nicht notwendigerweise auch das Vertragsende und ggf. möchte der Verantwortliche, dass der Auftragsverarbeiter die Daten über den Abschluss der Erbringung der Verarbeitungsleistungen hinaus aufbewahrt. Daher müssen ergänzend zu den gesetzlichen Verpflichtungen Vereinbarungen über die Löschung oder den Verbleib von Daten nach Vertragsende getroffen werden. Beispiele findet man in den Musterverträgen von bitkom, bvitg oder anderen[2].

Anforderung 15. Bei Beendigung des Vertragsverhältnisses löscht der Auftragsverarbeiter auf Wunsch des Verantwortlichen die (personenbezogenen) Daten, Dokumente und Kopien des Verantwortlichen oder er gibt auf Wunsch des Verantwortlichen die (personenbezogene) Daten, Dokumente und Kopien des Verantwortlichen an diesen zurück.

Dies gilt nicht, wenn der Auftragsverarbeiter gemäß der Vereinbarung oder gemäß geltendem Recht berechtigt oder verpflichtet ist, diese (personenbezogenen) Daten aufzubewahren und zu verarbeiten.

3.2 Vereinbarungen zur Informationsübertragung

Zwischen Verantwortlichen und Auftragsverarbeiter muss eine Vereinbarung existieren, welche die sichere Übertragung personenbezogener Daten während der Fernwartung behandelt.

[2] BvD, bvitg, DKG, GDD, GMDS: Mustervertrag zur Auftragsverarbeitung. [Online, zitiert am 2021-08-30]; Verfügbar unter https://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php
Bitkom: Begleitende Hinweise zu der Anlage Auftragsverarbeitung - Mustervertragsanlage: Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO). [Online, zitiert am 2021-08-30]; Verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Begleitende-Hinweise-zu-der-Anlage-Auftragsverarbeitung.html

3.2.1 Verantwortlichkeiten

Ein Fernwartungsprozess verpflichtet allein schon auf Grund der datenschutzrechtlichen Nachweispflicht, wer wann auf welche Daten Zugriff hatte, zur Protokollierung der Tätigkeiten der Fernwartung. Sowohl durch diese Protokollierung aber auch durch die Funktionalitäten einer Fernwartungssoftware liegt „technische Kontrolleinrichtungen“ vor, die gemäß § 87 Abs. 1 Nr. 6 BetrVG bzw. § 75 Abs. 3 Nr. 17 BPersVG mitbestimmungspflichtig ist. Entsprechend § 80 Abs. 2 BetrVG und § 68 Abs. 2 BPersVG muss der Arbeitgeber die Belegschaftsvertretung über die konkrete Ausgestaltung der Fernwartung und über die Funktionen der entsprechenden Software rechtzeitig und umfassend informieren.

Der Verantwortliche muss gewährleisten und garantieren, dass er befugt ist, den Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten durch Fernwartung zu beauftragen. Dazu muss er, wenn und wie gesetzlich vorgeschrieben, den betroffenen natürlichen Personen alle erforderlichen Hinweise vorlegen und falls notwendig die erforderlichen Einverständniserklärungen bei ihnen einholen. Bei der Fernwartung werden neben Patientendaten häufig auch Beschäftigtendaten des Verantwortlichen verarbeitet. Insbesondere können Softwarewerkzeuge zur Fernwartung ggf. auch zur Leistungskontrolle genutzt werden. Daher ist es zur Gewährleistung der rechtskonformen Fernwartung wichtig, dass auch die Beschäftigtendaten rechtmäßig verarbeitet werden, was in der Regel die Einbeziehung der Beschäftigtenvertretung durch den verantwortlichen beinhaltet.

Anforderung 16. Es ist Aufgabe des Verantwortlichen die Rechtmäßigkeit des Fernwartungsprozesses zu gewährleisten, wozu auch die Einbeziehung der Beschäftigtenvertretung gehört.

Es kann i.d.R. nicht 100%ig ausgeschlossen werden, dass während der Fernwartung auf personenbezogene Daten zugegriffen werden muss. Bei Daten von „normalen“ Kategorien kann dies ggf. durch Art. 6 Abs. 1 lit. f DS-GVO (ist zur Wahrung der berechtigten Interessen des Verantwortlichen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen) einen Erlaubnistatbestand darstellen. Bei Daten der besonderen Kategorien gemäß Art. 9 DS-GVO ist dies nicht möglich. Daher muss in diesen Fällen bei Fernwartung durch externes Personal ein Auftragsverarbeitungsvertrag abgeschlossen werden.

Anforderung 17. Zu jeder vertraglichen Vereinbarung bzgl. Fernwartung muss (mindestens) ein Vertrag zur Auftragsverarbeitung abgeschlossen werden, welcher den Anforderungen von Art. 28 DS-GVO genügt.

Entsprechend der DS-GVO muss der Verantwortliche einen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten haben. Für den Auftragsverarbeiter kann im Einzelfall aber nicht geprüft werden, ob tatsächlich ein solcher vorhanden ist. Daher wird vereinbart, dass Verantwortliche einen Auftragsverarbeiter nur dann beauftragen dürfen, wenn ein hinreichender Erlaubnistatbestand vorhanden ist.

Anforderung 18. Der Verantwortliche garantiert, dass er befugt ist, den Auftragsverarbeiter zur Verarbeitung personenbezogener Daten durch Fernwartung zu beauftragen und er, wenn notwendig, alle erforderlichen Einverständniserklärungen der betroffenen natürlichen Personen in seinem Unternehmen eingeholt hat.

Weiterhin sind die Art und der Umfang der Leistung vertraglich zu vereinbaren. Dies können z. B. Leistungen zur Mängelbehebung, zur Lieferung von Upgrades/Releases/Versionen oder auch Umsetzungs- und Installationsleistungen sein. Ggf. ist es sinnvoll, bei Beginn der vertraglichen Leistung die Erfassung der Ist-Situation zu dokumentieren und eine detaillierte Beschreibung des Soll-Zustands darzulegen. Insbesondere sind Regelungen bzgl. der Verantwortlichkeiten und Haftung bei Informationssicherheitsvorfällen zu treffen sowie die Zugangsmodalitäten zu beschreiben, d. h. Fragen wie „wann darf der Dienstleister sich selbst einwählen“ oder „wann muss der Verantwortliche freischalten“ sind zu klären.

Anforderung 19. In jeder vertraglichen Vereinbarung zur Fernwartung muss die zu erbringende Leistung vertraglich vereinbart sein, desgleichen Regelungen bzgl. der Verantwortlichkeiten und der Modalitäten bzgl. der Initialisierung des Fernwartungsvorganges.

Art. 29 DS-GVO legt fest, dass alle Personen, die Zugang zu personenbezogenen Daten haben, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten dürfen. Jedoch wird nicht festgelegt, dass der Auftragnehmer seinen Beschäftigten entsprechende Anweisungen erteilt. Da in Deutschland der Verantwortliche gegenüber den Beschäftigten des Auftragsverarbeiters arbeitsrechtlich keine Weisungsbefugnis hat, muss der Auftragnehmer das von ihm eingesetzte Personal dahingehend verpflichten, um zu gewährleisten, dass alle von ihm eingesetzten Personen personenbezogene Daten nur auf Weisung des Verantwortlichen verarbeiten entsprechend den vorliegenden Vereinbarungen und/oder anderweitigen schriftlich erteilten Anweisungen (sofern diese mit den Vereinbarungen konform sind) oder sofern dies gesetzlich erforderlich ist.

Anforderung 20. Alle vom Auftragsverarbeiter eingesetzten Personen, werden verpflichtet nur auf Weisungen des Verantwortlichen zu handeln.

Um die Beschäftigten des Auftragsverarbeiters vor unzulässigen Weisungen durch den Verantwortlichen zu schützen, muss der Verantwortliche sich verpflichten, keine gegen geltendes Recht verstoßenden Anweisungen zu erteilen.

Anforderung 21. Der Verantwortliche wird verpflichtet zu garantieren, dass seine Anweisungen nicht gegen geltendes Recht, einschließlich des Schutzes personenbezogener Daten, verstoßen oder bewirken, dass der Auftragsverarbeiter dadurch gegen geltendes Recht verstößt.

3.2.2 Nachverfolgbarkeit und Nichtabstreitbarkeit

Die Nachverfolgbarkeit und Nichtabstreitbarkeit bedingt eine sichere Identifikation der auf die personenbezogenen Daten zugreifenden Personen sowie eine entsprechende Protokollierung. Die Anforderungen bzgl. der sicheren Identifikation finden sich in Abschnitt 3.4.5.2, die bzgl. Protokollierung in Abschnitt 3.4.5.3.

3.2.3 Sichere Übertragung

Für jede Sitzung (auch Session genannt) muss eine Funktion implementiert sein, die verhindert, dass Sitzungen eines legitimen Benutzers von einem anderen Benutzer übernommen und/oder weitergeführt werden können. Ansonsten können Sitzungen u.U. von einem Angreifer weitergeführt werden und ggf. genutzt werden, um unberechtigten Zugriff auf ein System und damit auf die zu schützenden Daten zu erhalten. Ein entsprechender Schutz kann u.a. durch Nutzung der folgenden Maßnahmen implementiert werden:

- Verwendung des TCP-Protokolls (mit Sequence Number) und entsprechenden Filterlisten

- Nutzung kryptografischer Verfahren, z. B. auf Transportebene: SSL/TLS
- Aushandeln eines zufälligen und geheimen Wertes zwischen Sender und Empfänger (z. B. Session-ID, Zeitstempel)

Anforderung 22. Sitzungen müssen gegen eine unautorisierte Übernahme geschützt werden.

Um vor unberechtigter Einsichtnahme oder einem Abgriff von Daten zu schützen, müssen zur Übertragung hinreichend sichere Protokolle wie z. B. SSL/TLS-Envelopes oder SFTP genutzt werden.

Anforderung 23. Für die Kommunikation dürfen nur sichere Protokolle verwendet werden. Als sicher können Techniken angesehen werden, wenn diese eine dem Stand der Technik[3] entsprechende und vom BSI oder einer vergleichbaren Stelle empfohlene Verschlüsselung verwenden.

3.2.4 Kryptographische Methoden

Daten, welche nicht gegen eine unautorisierte Einsichtnahme und Veränderung geschützt werden, kann ein potenzieller Angreifer bei der Übertragung über eine Netzwerkverbindung mitlesen oder manipulieren. Daher müssen die Daten angemessen geschützt werden, auch bei temporärer Speicherung (temporärer Ordner, Web-Cache, usw.). Dementsprechend dürfen auch keine Übertragungsprotokolle genutzt werden, bei welchen die Übertragung nicht (z. B. FTP oder Telnet) oder unzureichend verschlüsselt (z. B. SSLv3 oder SSHv1) wird. Der Einsatz kryptografischer Verfahren gewährleistet einen Schutz gegen unautorisierte Einsichtnahme und Veränderung, aber nur wenn die Verfahren dem Stand der Technik entsprechen. Informationen zur Sicherheit von kryptografischen Verfahren finden sich insbesondere

- BSI: Technische Richtlinie 02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen[4].
  - BSI TR-02102-1: Bewertung der Sicherheit ausgewählter kryptographischer Verfahren, ermöglicht längerfristige Auswahl geeigneter Verfahren
  - BSI TR-02102-2: Empfehlungen bzgl. Einsatz TLS
  - BSI TR-02102-3: Empfehlungen bzgl. IPsec, und Internet Key Exchange
  - BSI TR-02102-4: Empfehlungen bzgl. SSH

Anforderung 24. Schutzbedürftige Daten dürfen nur verschlüsselt übertragen werden.

Anforderung 25. Es werden hinreichend starke kryptografische Verfahren zur Verschlüsselung verwendet, die mindestens dem Stand der Technik entsprechen. Als dem Stand der Technik

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI) - Branchenspezifische Sicherheitsstandards: „‘Stand der Technik‘ st ein gängiger juristischer Begriff. Die technische Entwicklung ist schneller als die Gesetzgebung. Daher hat es sich in vielen Rechtsbereichen seit vielen Jahren bewährt, in Gesetzen auf den "Stand der Technik" abzustellen, statt zu versuchen, konkrete technische Anforderungen bereits im Gesetz festzulegen. Was zu einem bestimmten Zeitpunkt "Stand der Technik" ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und Normen von beispielsweise DIN, ISO, DKE oder ISO/IEC oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln.“ [Online, zitiert am 2021-08-30]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html

[4] [Online, zitiert am 2021-08--30];
Verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

entsprechend können kryptografische Verfahren angesehen werden, die vom BSI oder einer vergleichbaren Stelle für einen entsprechenden Einsatz empfohlen werden.

Liegt die Schlüsselgewalt sowie die Kontrollmöglichkeit nicht in der Hand der Kommunikationspartner, sind Man-in-the-middle-Attacken realisierbar

Anforderung 26. Private Schlüssel müssen sich ausschließlich in der Verfügungsgewalt des jeweiligen Kommunikationspartners befinden, ebenso müssen alle für die Verbindung genutzten Zertifikate fälschungssicher und überprüfbar sein. Sowohl die Überprüfbarkeit wie auch die Fälschungssicherheit muss nachgewiesen werden können.

3.3 Richtlinien für die Informationsübertragung

Bei der Übertragung von Daten müssen die nachfolgend dargestellten Grundsätze erfüllt werden.

3.3.1 Authentifizierung

Die Anforderungen bzgl. der sicheren Identifikation der auf die personenbezogenen Daten zugreifenden Personen wird im Abschnitt 3.4.5.2 dargestellt.

3.3.2 Datenversand

Werden im Rahmen der Wartung Informationen postalisch zugesandt (beispielsweise Hardware, in denen Speichermedien mit personenbezogenen Daten enthalten sind), so ist bei dem Versand die korrekte Adressierung wie auch die sichere Beförderung durch Auswahl eines entsprechenden Dienstleisters zu gewährleisten.

Anforderung 27. Bei einem postalischen Versand personenbezogener Daten ist immer die korrekte Adressierung zu gewährleisten. Für den Transport selbst dürfen nur Dienstleister ausgewählt werden, bei denen ein sicherer Transport anzunehmen ist. Der Verantwortliche wie auch der Auftragsverarbeiter bei einem Einsatz von Unterauftragnehmern muss die sorgfältige Auswahl des Dienstleisters und insbesondere die bei der Auswahl nachgewiesene Sicherheit des Transportes nachweisen.

Diese Anforderung gilt auch im Rahmen von elektronischen Übertragungen. Auch hier müssend die Kommunikationspartner, z.B. Server oder Clients, sicher identifiziert werden. Dies kann z.B. durch elektronische Zertifikate erfolgen.

Anforderung 28. Bei elektronischer Übertragung personenbezogener Daten müssen die elektronischen Kommunikationsparteien identifiziert werden. Eine zertifikatsbasierte Authentisierung muss gegenüber Pre-Shared Key (PSK) Verfahren bevorzugt werden.

Auch die elektronische Übertragung muss geschützt werden. (Näheres hierzu siehe Kapitel 3.2.3 auf Seite 15.) Sowohl um die Gewissheit hinsichtlich des Ursprungs der Nachrichten zu erhalten als auch um die Integrität überprüfen zu können, müssen Message Authentication Codes (MAC) eingesetzt werden.

Anforderung 29. Um Ursprung und Integrität elektronischer Nachrichten überprüfen zu können, müssen Message Authentication Codes eingesetzt werden. Hierbei dürfen nur vom BSI empfohlene Algorithmen[5] verwendet werden.

3.3.3 Schutzmaßnahmen

Grundsätzlich muss auf allen an der Fernwartung beteiligten elektronischen Geräten ein dem Stand der Technik genügender Schutz vor Angriffen, Schadsoftware, etc. vorhanden sein. Dazu zählen insbesondere:

- Virenscanner als Schutz vor Schadsoftware
- Firewalls, um insbesondere auch einen Ausfall der Fernwartung durch Denial of Service Angriffen zu verhindern
- Spamfilter als Schutz vor Mail-Angriffen, die ggf. Schadsoftware enthält, z.B. um Passwortdiebstahl zu ermöglichen.

Anforderung 30. Alle an der elektronischen Kommunikation beteiligten Geräte müssen über einen dem Stand der Technik genügenden Schutz vor Schadsoftware verfügen.

Anforderung 31. Insbesondere muss, sofern die Geräte eine entsprechende Funktionalität bereitstellen und eine entsprechende Installation erlaubt ist, eine Antivirus/Antimalware Software eingestellt werden, dass die Geräte in kurzen regelmäßigen Abständen komplett überprüft werden und die Antivirus/Antimalware Software aktuell gehalten wird.

Anforderung 32. Die Sicherheitsmechanismen des BIOS/EFI müssen vorhanden sein und zum Schutz von unerwünschten Änderungen des BIOS/EFI genutzt werden.

Anforderung 33. Sicherheitsfunktionen der Geräte wie DEP, ASLR, etc. sollten, wenn vorhanden, genutzt werden, wenn sowohl das Betriebssystem als auch die Anwendungen derartige Funktionen unterstützen.

Bei elektronischen Datenübermittlungen kann das Abfangen von Nachrichten durch Unbefugte nicht sicher verhindert werden. Daher müssen die in den elektronischen Nachrichten enthaltenen Informationen geschützt werden. Dies geschieht durch die Verschlüsselung der schutzbedürftigen Daten (siehe Kapitel 3.2.4).

Anforderung 34. Es dürfen nur standardisierte kryptographische Verfahren eingesetzt werden. Die Verfahren sollten durch mindestens eine anerkannte Institution wie beispielsweise BSI oder NIST empfohlen werden.

Damit eine sichere Identifikation des Absenders möglich sowie Manipulationen der Informationen erkennbar ist, sollten elektronische Signaturen eingesetzt werden.

Anforderung 35. Um den Absender der Nachrichten sicher identifizieren und Manipulationen der Informationen sicher erkennen zu können, sollte eine elektronische Signatur verwendet

[5] Hinweise zur Auswahl eines Verfahrens siehe BSI Technische Richtlinie 02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ ([Online, zitiert am 2021-08-30]; Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=12)

werden. Wird eine elektronische Signatur verwendet, dürfen für die Erzeugung der Signatur nur vom BSI empfohlene Algorithmen[6] verwendet werden.

3.3.4 Home Office, Mobile Office

Die fortschreitende Digitalisierung macht auch vor der Arbeitswelt nicht Halt. Unternehmen müssen heute Beschäftigten beim Kampf um die besten Arbeitskräfte u.a. flexible Arbeitsmodelle wie Home Office und mobile Telearbeit ermöglichen. Damit ist jedoch der feste Arbeitsplatz beim Arbeitgeber inklusive der damit verbundenen Kontrolle der Arbeitsumgebung nicht mehr gegeben. Da gem. Art. 4 Ziff. 7 DS-GVO der Verantwortliche über Zwecke und Mittel der Verarbeitung entscheidet und Home Office ein Mittel der Verarbeitung darstellt, ist eine entsprechende Tätigkeit nur mit dessen Genehmigung statthaft. Insbesondere verlangt Art. 29 DS-GVO, dass dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, dürfen, so dass auch aus diesen Gründen eine Zustimmung erforderlich ist. Zudem muss der Verantwortliche nach Art. 32 Abs. 2 DS-GVO bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken der Verarbeitung berücksichtigen und daher auch die Risiken des Home Office beurteilen.

Anforderung 36. Home Office und mobile Telearbeit ist nur mit Zustimmung des Verantwortlichen gestattet.

Gerade bei der Verarbeitung von sensiblen Daten der in Art. 9 Abs. 1 DS-GVO genannten Datenkategorien ist eine entsprechende Absicherung der Arbeitsumgebung unabdingbar.

Anforderung 37. Home Office und mobile Telearbeit darf nur unter denselben Bedingungen wie die Arbeit innerhalb der betrieblichen Umgebung erlaubt werden. Insbesondere ist mindestens dasselbe Schutzniveau wie in der betrieblichen Umgebung zu gewährleisten.

Einige Aufsichtsbehörden verlangen bei einer Verarbeitung in einer Privatwohnung oder entsprechenden Umgebungen, dass zuvor der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicher zu stellen ist[7]. Die DS-GVO fordert jedoch keine Kontrolle, sondern hinreichend Garantien, „dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person“ gewährleisten. Dementsprechend ist für Routinekontrollen ein Zugang insbesondere unter Beachtung von Art. 13 GG[8] nicht zwingend erforderlich. Im Falle von Verletzungen des Schutzes personenbezogener Daten können Kontrollen jedoch erforderlich sein, insbesondere auch Kontrollen durch Datenschutz-Aufsichtsbehörden. Daher muss eine Regelung zum Zugang zu den Räumlichkeiten bei Telearbeit vorhanden sein.

[6] Bzgl. der empfohlenen Algorithmen siehe Kapitel 5.4 in der Technischen Richtlinie 02102-1 des BSI ([Online, zitiert am 2021-08-30]; Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf)

[7] Die Landesbeauftragte für den Datenschutz Niedersachsen: Formulierungshilfe zur Auftragsverarbeitung nach Art. 28 DS-GVO (Seite 5). [Online, zitiert am 2021-08-30]; Verfügbar unter https://www.lfd.niedersachsen.de/download/127630

[8] Grundgesetz für die Bundesrepublik Deutschland: Art. 13. [Online, zitiert am 2021-08-30]; Verfügbar unter https://www.gesetze-im-internet.de/gg/art_13.html

Anforderung 38. Der Zugang zu den Räumlichkeiten, in denen Telearbeit vorgenommen wird, muss geregelt sein. Insbesondere müssen Regelungen vorhanden sein, welche der Datenschutz-Aufsichtsbehörde im Bedarfsfall den Zugang zu den Räumlichkeiten ermöglicht.

3.4 Umgang mit datenschutzrechtlichen Pflichten

3.4.1 Informationspflicht

Aus Artt. 13, 14 DS-GVO resultieren Informationspflichten, welche der Verantwortliche wahrzunehmen hat. Diese Pflichten gelten bei jeder Verarbeitung personenbezogener Daten, somit insbesondere auch bei Fernwartung. D. h.

- Werden personenbezogene Daten bei der betroffenen Person erhoben, so muss der Verantwortliche der betroffenen Person die Informationen gem. Art. 13 DS-GVO mitteilen, es sei denn, die Person verfügt bereits über die Informationen. Die Informationen müssen der betroffenen Person zum Zeitpunkt der Erhebung zur Verfügung gestellt werden.
- Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so muss der Verantwortliche der betroffenen Person die Informationen gem. Art. 14 DS-GVO mitteilen, es sei denn, die Person verfügt bereits über die Informationen oder es liegt eine weitere Ausnahme gem. Art. 14 DS-GVO vor. Die Informationen müssen der betroffenen Person zu dem frühesten Zeitpunkt zur Verfügung gestellt werden, der sich aus den folgenden Bedingungen ergibt:
  - Innerhalb einer angemessenen Frist nach Erlangung der Daten, aber auf jeden Fall innerhalb eines Monats.
  - Falls die Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens bei der ersten Mitteilung an sie.
  - Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens bei erster Offenlegung.
- Die Informationen müssen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermittelt werden.
- Sollen die Daten für einen anderen Zweck weiterverarbeitet werden als den, für den sie erhoben wurden, so muss die betroffene Person vor der Weiterverarbeitung informiert werden.

Anforderung 39. Der Verantwortliche muss nachweisen können, dass und ggf. in welcher Version er die Informationen gem. Artt. 13, 14 DS-GVO der jeweiligen betroffenen Person zur Verfügung gestellt hat.

3.4.2 Auskunftspflicht

Das Auskunftsrecht der betroffenen Person (Art. 15 DS-GVO) bezieht sich neben Informationen zur Verarbeitung auch auf die Personen bzw. Kategorien von Personen die Einsicht in die Daten haben oder haben könnten sowie auf die Verarbeitung in Drittstaaten.

Anforderung 40. Der betroffenen Person müssen auf deren Nachfrage alle Informationen mitgeteilt werden, die eine faire und transparente Verarbeitung aus Sicht der betroffenen Person ermöglichen. Insbesondere muss den Anforderungen von Art. 15 DS-GVO genügt werden.

Anforderung 41. Die Informationen müssen unentgeltlich zur Verfügung gestellt werden.

3.4.3 Privacy by Design

Die Datenschutzgrundverordnung fordert, dass „sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen“ die Datenschutzgrundsätze gewährleistet werden. Dies kann nur der Verantwortliche selbst gewährleisten, da der Auftragsverarbeiter nur im Rahmen der Weisungen des Verantwortlichen tätig wird, d. h. zum Zeitpunkt der Festlegung der Mittel noch gar nicht eingebunden war.

3.4.4 Datenschutz-Folgenabschätzung

Eine Fernwartung ist immer nur ein Teilaspekt bei der Nutzung eines Informationssystems. Ist für die gesamte Verarbeitung eine Datenschutz-Folgenabschätzung erforderlich, so muss diese Datenschutz-Folgenabschätzung auch die Fernwartung selbst beinhalten. D. h. entweder für die Fernwartung ist keine getrennte Datenschutz-Folgenabschätzung erforderlich oder die Datenschutz-Folgenabschätzung erfolgte bereits bei der Betrachtung des eigentlichen Verarbeitungsverfahrens.

3.4.5 Sicherheit der Verarbeitung

Die Sicherheit der Verarbeitung muss bei der Fernwartung zu jedem Zeitpunkt gewährleistet sein. Neben dem Schutz der Daten während der Informationsübertragung (siehe Abschnitt 3.3) muss während der Verarbeitung das Schutzniveau ebenso hoch sein, wie bei einer Verarbeitung ohne Fernwartung.

Anforderung 42. Bei jeder Fernwartung muss während der Verarbeitung das Schutzniveau mindestens dem Stand des Schutzniveaus der Verarbeitung ohne Fernwartung entsprechen.

3.4.5.1 Pseudonymisierung / Anonymisierung

Art. 32 DS-GVO schreibt als Schutzmaßnahmen insbesondere Pseudonymisierung und Verschlüsselung vor. Daher sind diese Maßnahmen grundsätzlich umzusetzen, außer dies ist zur Erreichung des Zweckes nicht möglich. In diesem Fall muss eine Begründung erfolgen. Z. B. kann eine Pseudonymisierung je nach Anwendungsfall eine Gefährdung von Patienten beinhalten, weil Daten bei einer Behandlung ggf. nicht dem richtigen Patienten zugeordnet werden.

Anforderung 43. Pseudonymisierung und Verschlüsselung müssen zum Schutz personenbezogener Daten eingesetzt werden. Sollte dies nicht erfolgen, muss diese Entscheidung begründet werden.

3.4.5.2 Vertraulichkeit

Nur wenn gewährleistet ist, dass die einen Fernzugriff durchführende Person sicher identifiziert werden kann, können im Bedarfsfall Zugriffe auf sensible/kritische Daten nachvollzogen werden. Daher müssen Verantwortlicher und/oder Auftragsverarbeiter über ein Identitätsmanagementprozess verfügen, mit dem die Identitäten der Nutzer mit Zugang zu Systemen verwaltet werden.

Anforderung 44. Es existiert ein Identity Management inkl. eines zentralen Benutzermanagements, welches bei jedem Fernwartungsvorgang die Identität der zugreifenden Personen gewährleistet.

Anforderung 45. Es müssen Benutzerkonten verwendet werden, welche die eindeutige Identifizierung des Benutzers ermöglichen.

Fernzugriffsmöglichkeiten stellen aufgrund der Zugriffsmöglichkeiten von außerhalb des Unternehmens grundsätzlich eine potenzielle Sicherheitslücke dar. Eine Dokumentation der externen Verbindungen ist eine grundlegende Anforderung, um den Sicherheitsstatus und die Risiken für die internen Netze beurteilen zu können. Nur so kann eine Übersicht gewährleistet werden, welche legitimen externen Zugriffsmöglichkeiten existieren. Sämtliche Fernzugriffsmöglichkeiten werden im Rahmen eines Sicherheitsmanagements erfasst. Dies beinhaltet die Art des Zugangs, die betroffenen Systeme, die berechtigten Personen sowie die zugehörigen Vorgaben und Prozesse. Da bei einem Verantwortlichen mehrere Fernwartungszugriffe von verschiedenen Auftragsverarbeitern vorkommen können, der Verantwortliche aber die Verantwortung für die Sicherheit seiner Systeme haben muss, kann nur der Verantwortliche ein derartiges Verzeichnis, welches die Übersicht über alle Fernwartungsvorgänge beinhaltet, führen. Ob der jeweilige Fernwartungsvorgang durch den Verantwortlichen oder Auftragsverarbeiter oder direkt automatisiert erfolgt, kann nur im jeweiligen Einzelfall festgelegt werden.

Anforderung 46. Es existiert ein Verzeichnis der Fernzugriffsmöglichkeiten, in welchem jeder Fernwartungsvorgang aufgezeichnet wird. Es wird festgelegt, welche Vertragspartei dieses Verzeichnis führt.

Die Berechtigungen müssen soweit eingeschränkt werden, dass ein Benutzer nur auf Daten zugreifen und Funktionen nutzen kann, die er im Rahmen seiner Arbeit benötigt. Entsprechende Berechtigungen sind auch für den Zugriff auf Dateien, die Bestandteil des Betriebssystems oder von Anwendungen sind oder von diesen erzeugt werden (z. B. Konfigurations- und Protokollierungsdateien), zu vergeben. Weiterhin muss auch die Ausführung von Anwendungen mit möglichst niedrigen Berechtigungen erfolgen. Anwendungen sollten nicht mit Administrator- oder Systemberechtigungen ausgeführt werden, wenn dies nicht zwingend erforderlich ist. Sofern für ausgewählte Tätigkeiten zusätzliche Berechtigungen (z. B. Administratorberechtigung) erforderlich sind, dürfen diese nur zeitbegrenzt durch den Auftraggeber erteilt werden. Dabei erlaubt nur ein rollenbasierter Zugriff auch bei einer Vielzahl von Benutzerkonten den Überblick, welche Rechte vergeben wurden.

Anforderung 47. Die Berechtigungen von Benutzerkonten und Anwendungen müssen auf ein für deren Aufgaben notwendiges Minimum reduziert werden.

Anforderung 48. Der Zugang eines Nutzers der Fremdfirma muss rollenbasiert erfolgen.

Bei der Installation von Betriebssystemen werden i.d.R. vordefinierte und nicht genutzte Benutzerkonten (z. B. Gast) eingerichtet, die teilweise ohne, teilweise mit bekannten Passwörtern vorkonfiguriert sind. Diese Zugangsdaten sind allgemein bekannt und bieten potenziellen Angreifern die Möglichkeit, sich anzumelden und mit den Rechten dieser Konten zu arbeiten. Diese Standardbenutzer müssen daher entweder gelöscht oder deaktiviert werden. Sollten diese Maßnahmen nicht umsetzbar sein, muss das entsprechende Benutzerkonto für einen Fernzugriff gesperrt werden. Weiterhin müssen gesperrte und deaktivierte Benutzerkonten mit einem möglichst komplexen Passwort (12 Zeichen und mehr, Nutzung von Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen) versehen werden, so dass auch im Falle einer Fehlkonfiguration die unberechtigte Nutzung eines solchen Benutzerkontos verhindert wird.

Anforderung 49. Vordefinierte und nicht benötigte Benutzerkonten müssen gelöscht oder deaktiviert werden.

Häufig existieren auf Systemen vom Hersteller, Entwickler oder Lieferanten vorkonfigurierte Authentisierungsmerkmale wie Passwörter und kryptographische Schlüssel. Solche Authentisierungsmerkmale müssen in eigene, Dritten nicht bekannte Merkmale geändert werden, um Angreifern den Zugang zu erschweren.

Anforderung 50. Vordefinierte Authentisierungsmerkmale müssen geändert werden.

Anforderung 51. Die Nutzung und der Zugriff auf schutzbedürftige Funktionen und Informationen, dürfen nicht ohne erfolgreiche Authentifizierung und Autorisierung möglich sein.

Das Betriebssystem/die Anwendung muss über eine Funktion verfügen, die es dem angemeldeten Benutzer ermöglicht, sich jederzeit abzumelden. Die Fortführung einer abgemeldeten Sitzung darf nicht ohne erneute und erfolgreiche Authentifizierung des Benutzers möglich sein.

Anforderung 52. Das System muss es dem Benutzer ermöglichen, die Fernwartungssitzung zu beenden.

Eine starke Authentifizierung erfolgt immer auf Basis mehrerer (mindestens zwei) Merkmale wie z. B. Besitz und Wissen oder auf einer einmaligen, dem Nutzer eigenen Eigenschaft.

Anforderung 53. Bei besonders sensiblen Daten wie z. B. Gesundheitsdaten sollte nach Möglichkeit ein Zwei-Faktor-Verfahren als Authentisierungsmechanismus einzusetzen.

Triviale und zu kurze Passwörter sind anfällig gegen Brute-Force- und Wörterbuch-Angriffe und sind von einem Angreifer leicht zu ermitteln. Ein einmal ermitteltes Passwort kann dann von einem Angreifer für den unautorisierten Zugriff auf das System und dessen Daten genutzt werden. Passwörter mit der in der Anforderung beschriebenen Komplexität bieten eine hohe Robustheit gegen Angriffe bei gleichzeitig akzeptabler Benutzerfreundlichkeit.

Anforderung 54. Falls Passwörter als Authentisierungsmerkmal genutzt werden, müssen diese dem Stand der Technik entsprechen. Jede an der Fernwartung beteiligte Partei führt den Nachweis, dass die Regeln zur Passwortvergabe dem Stand der Technik entsprechen[9].

Nur durch die Möglichkeit, dass ein Benutzer sein Authentisierungsmerkmal jederzeit selbsttätig ändern kann, ist eine zeitnahe Änderung möglich, wenn der Benutzer den Verdacht hat, dass dieses in den Besitz Dritter gelangt sein könnte.

Anforderung 55. Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss eine Änderung des eigenen Passwortes jederzeit durch den Benutzer möglich sein.

Ohne entsprechenden Schutz kann ein Angreifer durch bloßes Durchprobieren von Wörterbuchlisten oder automatisch erzeugten Zeichenkombinationen versuchen, ein Passwort zu ermitteln, um so das entsprechende Benutzerkonto missbräuchlich zu nutzen.

[9] Bzgl. der Hinweise, wie Passwörter vergeben werden sollten, ist das National Institute of Standards and Technology (NIST) weltweit führend. Unter Digital Identity Guidelines (Online, zitiert am 2021-08-30]; Verfügbar unter https://pages.nist.gov/800-63-3/) finden sich 4 Regelwerke, „Authentication and Lifecycle Management“ (Online, zitiert am 2021-08-30]; Verfügbar unter https://doi.org/10.6028/NIST.SP.800-63b) beinhaltet im Kapitel 5.1.1 „Memorized Secrets“ sowie im Appendix A „Strength of Memorized Secrets“ Hinweise zur Passortvergabe

Anforderung 56. Falls Passwörter als Authentisierungsmerkmal genutzt werden, muss ein Schutz gegen Wörterbuch- und Brute-Force-Angriffe vorhanden sein, der das Erraten von Passwörtern stark erschwert. Jede an der Fernwartung beteiligte Partei führt den Nachweis, dass ein entsprechender Schutz vorhanden ist.

Damit eine andere Person bei der Eingabe eines Passwortes dieses nicht zufällig oder absichtlich vom Bildschirm ablesen kann, muss das Passwort bei der Eingabe oder Darstellung unkenntlich gemacht werden. Typischerweise werden die einzelnen Zeichen des Passwortes durch ein Zeichen wie „*“ ersetzt. Unter bestimmten Voraussetzungen kann es zulässig sein, dass ein einzelnes Zeichen bei der Eingabe kurz angezeigt wird, allerdings darf niemals das ganze Passwort im Klartext auf dem Display angezeigt werden.

Anforderung 57. Falls Passwörter als Authentisierungsmerkmal genutzt werden, darf deren Darstellung nicht im Klartext erfolgen.

Sowohl bei der Installation von Betriebssystemen wie auch von Softwareanwendungen werden regelmäßig Dienste und Protokolle installiert und aktiviert, die für den Anwendungsfall nicht notwendig sind. Jeder Dienst wie auch jedes Protokoll stellt eine Sicherheitslücke dar und muss daher desinstalliert oder zumindest deaktiviert werden, wenn er nicht benötigt wird.

Anforderung 58. Nicht benötigte Dienste und Protokolle müssen deaktiviert werden.

Schwachstellen ermöglichen Angreifern Zugriff auf zu schützende Informationen. Komponenten, welche eine Schwachstelle aufweisen, dürfen daher nicht installiert oder verwendet werden. Ausnahme hiervon sind Komponenten, für die bereits eine Maßnahme zum Beheben der Schwachstelle, wie z. B. ein Patch, ein Update oder ein Workaround, existiert, sofern diese Maßnahme auf dem System umgesetzt wurde.

Anforderung 59. Bekannt gewordene Schwachstellen in der Software oder Hardware des Systems müssen gegen Missbrauch abgesichert werden. Die Schwachstellen müssen so schnell wie möglich beseitigt werden. Für die Dauer des Bestehens von Schwachstellen muss der Verantwortliche an Hand einer Risikoanalyse entschieden werden, ob der Betrieb aufrechterhalten oder eingestellt werden muss.

3.4.5.3 Integrität

Zur Gewährleistung der Integrität müssen unautorisierter Modifikationen von Informationen verhindert werden. Dies kann niemals vollständig gewährleistet werden, daher müssen Methoden zur Erkennung unerlaubter bzw. unerwünschter Änderungen vorhanden sein.

Eine zustandsorientierte (stateful) Firewall entspricht dem Stand der Technik und ist daher das Mittel der Wahl zum Schutz dieser Netzschicht.

Anforderung 60. Die Zugangsplattform für die Fernwartung muss in der DMZ liege, die DMZ muss mit dem Stand der Technik entsprechenden Firewalls sowohl nach außen zum Internet wie auch nach innen geschützt werden. Den Nachweis für die Konfiguration des sicheren Fernwartungszugangs führt jede an der Fernwartung beteiligte Partei.

Grundsätzlich kann jede Datei Malware enthalten und muss daher daraufhin überprüft werden.

Anforderung 61. Jeder Dateiaustausch muss mit einem aktuellen Malware-Scanner überprüft werden. Vertraglich muss im Leistungsvertrag oder im Vertrag zur Auftragsverarbeitung festgelegt werden, wo die Prüfung erfolgt.

Bei einer Fernwartungssitzung ist grundsätzlich ein Zugriff auf kritische und/oder sensible Daten nicht auszuschließen und eine detaillierte Protokollierung („Audit-Trail“), anhand dessen man die Vorgänge im Rahmen der Fernwartung nachvollziehen kann, ist daher zwingend erforderlich. Die Protokolldaten liefern auch wichtige Informationen, wenn es zu Sicherheitsvorfällen kommt. Für korrekte Datums- und Zeitinformationen müssen alle protokollierenden Systeme an einen Dienst zur Zeitsynchronisation angebunden sein.

Protokollierung bedeutet in diesem Sinne die Erfassung des Textinhalts sowie – soweit möglich - des visuellen Inhalts der Fernwartungssitzung, einschließlich aller Metadaten und übertragenen Dateien (binäre Erfassung). Die Aufzeichnung besteht idealerweise in einem Film, welcher die Session mit allen Interaktionen in Echtzeit zeigt, sowie Kopien der übertragenen Dateien.

Anforderung 62. Die Fernwartungssitzung muss protokolliert werden.

Anforderung 63. Jeder erfolgreiche/fehlgeschlagene Versuch des Zugangs muss vom System protokolliert werden.

Anforderung 64. Für erfolgreiche Versuche des Zugangs muss das Sitzungs-Protokoll definierte Parameter enthalten wie:

- **Zeitzone, Datum und Uhrzeit des Sitzungs-Beginns sowie des Sitzungs-Endes**
- **Name und IP-Adresse der zugreifenden Quelle**
- **Account-Name (Nutzer) bzw. ID der Schnittstelle**
- **Name und IP-Adresse des Zielobjekts (Zielsystem/Anwendung)**
- **Name und TCP-Port des Zielservice**
- **Aktion (Sitzung hergestellt/beendet, Sitzungsanfrage zurückgewiesen.**

Nur Protokolle, deren Authentizität gewährleistet ist, bieten die notwendige Sicherheit, dass die festgehaltenen Ereignisse auch so geschehen sind. Eine wichtige Anforderung, um dies zu gewährleisten, ist eine separate Speicherung, so dass der Zugriff auf die Daten entsprechend begrenzt werden kann. Die Übertragung der Protokolle/Aufzeichnungen zum Protokollserver muss auf sichere Weise erfolgen (z. B. über sftp). Das Zeitintervall zwischen den Protokollübertragungen muss so kurz wie möglich sein.

Anforderung 65. Sitzungs-Protokolle und Sitzungs-Aufzeichnungen müssen in einem separaten Protokollarchiv gespeichert werden.

Anforderung 66. Sitzungs-Protokolle und -Aufzeichnungen müssen manipulations-/ fälschungssicher aufbewahrt werden.

Anforderung 67. Sitzungs-Protokolle und -Aufzeichnungen müssen gelöscht werden, sobald der Zweck es zulässt und keine gesetzlichen Aufbewahrungsfristen eine längere Aufbewahrung erfordern.

3.4.5.4 Verfügbarkeit

Fernzugriffsmöglichkeiten werden nur eingerichtet, wenn dafür eine Erforderlichkeit besteht. Dies bedingt jedoch, dass die Fernzugriffsmöglichkeiten insbesondere auch für zeitkritische Zugriffe im Bedarfsfall funktionieren müssen. Für einen Fernwartungsvorgang muss dementsprechend die Kritikalität bestimmt werden, d. h. es müssen konkrete Mindestangaben zur Verfügbarkeit definiert werden. Um die Verfügbarkeit zu gewährleisten, ist weiterhin eine regelmäßige Prüfung – insbesondere nach Konfigurationsänderungen der Firewall – unabdingbar. Je nach Konfiguration des Fernwartungsvorganges kann dies Auftraggeber oder der Auftragnehmer oder nur beide Zusammen die Prüfung durchführen; dies ist festzulegen.

Anforderung 68. Für einen Fernwartungsvorgang muss die Kritikalität bestimmt werden, d. h. es müssen konkrete Mindestangaben zur Verfügbarkeit definiert werden.

Anforderung 69. Es erfolgt eine regelmäßige Prüfung der Funktionsfähigkeit der Fernwartungssoftware. Vertraglich wird festgelegt, wer diese Prüfung in welchen Abständen durchführt und Erfolg oder Misserfolg dokumentiert.

3.4.5.5 Belastbarkeit/ Resilienz

Um die Ausfallsicherheit zu gewährleisten, müssen die für den Einzelfall erforderlichen Maßnahmen ergriffen werden. Nicht bei jeder Fernwartung muss hohe Verfügbarkeit gewährleistet werden, sondern die Verfügbarkeit muss in Abhängigkeit der Kritikalität der Geschäftsanwendung festgelegt werden. Beispielsweise ist eine Fernwartung, die zur Gewährleistung der Patientenversorgung erforderlich ist, bzgl. Verfügbarkeit anders zu bewerten, als eine Fernwartung, welche zur Abwicklung der Gehaltszahlung von Beschäftigten benötigt wird. Wo die eine Funktionalität unverzichtbar ist, kann bei der anderen ggf. 1 Tag Verzögerung akzeptabel sein.

Anforderung 70. Die Verfügbarkeit der Fernwartung inklusive der größtmöglichen Zeitdauer der Wiederherstellbarkeit der Verfügbarkeit muss festgelegt werden.

Anforderung 71. Es wurden Single-Points-of Failure identifiziert und durch angemessene Maßnahmen behandelt.

Anforderung 72. Es wurde festgelegt, welche Personen bei welcher Störung oder welchem Ausfall zu benachrichtigen sind.

Anforderung 73. Es existiert ein Notfallplan, wie bei Ausfall der Fernwartung zu verfahren ist.

Abhängig von der für den jeweiligen Einzelfall festgelegten Kritikalität sind nachfolgende Anforderungen als Mindeststandard anzusehen.

Anforderung 74. Es existiert eine unterbrechungsfreie Stromversorgung, welche die Verfügbarkeit der Fernwartung auch bei Ausfällen der Stromversorgung gewährleistet.

Anforderung 75. Es existieren redundante Systeme, die eine Verfügbarkeit der Fernwartung auch bei Ausfall einzelner Systeme gewährleisten.

Anforderung 76. Virenscanner werden zum Schutz der zur Fernwartung genutzten Systeme eingesetzt.

Anforderung 77. Eine Firewall wird zum Schutz des bei der Fernwartung genutzten Zugangs eingesetzt.

3.4.5.6 Wiederherstellbarkeit

Für einen Fernwartungsvorgang müssen Maßnahmen vorhanden sein, welche gewährleisten, dass die Funktionalität der Fernwartung bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann.

Anforderung 78. Es wurden die maximalen Ausfallzeiten für die eingesetzten IT-Systeme festgelegt.

Anforderung 79. Die Personen, die bei einer Störung oder einem Ausfall zu benachrichtigen, sind wurden bestimmt, ihre Kontaktdaten stehen allen an der Verarbeitung beteiligten Personen zur Verfügung.

Anforderung 80. Es wurden alle Konfigurationsparameter der benutzten Betriebssysteme und Anwendungen sowie der eingesetzten Protokolle dokumentiert, so dass eine schnellstmögliche Wiederherstellbarkeit des Fernwartungssystems gegeben ist.

Anforderung 81. Ist eine Hochverfügbarkeit und eine möglichst unverzügliche Wiederherstellbarkeit notwendig, sind die folgenden Anforderungen verpflichtend:

- **a) Es wird ein Netzwerk-Monitoring eingesetzt, welches alle für die Fernwartung relevanten Server, Dienste und Prozesse überwacht und Abweichungen zuverlässig meldet.**
- **b) Es existiert eine redundante Benachrichtigungsfunktion (z.B. Mail, SMS), welche über Störungen/Ausfälle relevanter IT-Systeme informiert.**
- **c) Eine unterbrechungsfreie Stromzufuhr muss einsatzbereit zur Verfügung stehen.**
- **d) Bei Ausfällen übernehmen redundante Stand-By-Systeme wechselseitig die Funktionalitäten.**

3.4.5.7 Auditierung

Die Wirksamkeit und Verfügbarkeit der Maßnahmen müssen regelmäßig geprüft werden. D. h. es müssen regelmäßig Tests erfolgen, ob ein Backup sich wieder einspielen lässt, ob eine unterbrechungsfreie Stromversorgung anspringt usw.

Anforderung 82. Die Wirksamkeit aller Maßnahmen, welche zur Aufrechterhaltung der Funktionalität der Fernwartung getroffen wurden, müssen in regelmäßigen Abständen geprüft werden.

3.4.6 Verarbeitung im Ausland

Der Auftragnehmer ist gegebenenfalls bei der Erbringung der Leistungen auf die Unterstützung von verbundenen Unternehmen oder Dritten, die als Unterauftragsverarbeiter agieren, angewiesen. Diese Unterauftragsverarbeitung erfolgt möglicherweise an Standorten außerhalb des EWR.

3.4.6.1 Verarbeitung im europäischen Ausland

Entsprechend Art. 1 Abs. 3 DS-GVO darf der „freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden“. Dementsprechend kann eine Fernwartung aus jedem

Ort erbracht werden, in welchem die DS-GVO ihre direkte Wirkung entfaltet, d. h. innerhalb des EWR ist die Verarbeitung vorbehaltlich der Gewährleistung der Anforderungen der DS-GVO statthaft.

Bei der Verarbeitung von Daten, die durch § 203 StGB geschützt sind, ist ggf. zu prüfen, ob der strafrechtliche Schutz bei einer Verarbeitung aus dem europäischen Ausland heraus ebenfalls gewährleistet ist.

3.4.6.2 Verarbeitung in Drittländern

Eine Verarbeitung personenbezogener Daten der besonderen Kategorie nach Art. 9 DS-GVO im Rahmen von Fernwartung sollte nach Möglichkeit vermieden werden. Gerade bei Software, die in Drittländern entwickelt wurde bzw. weiterentwickelt wird, lässt sich dies jedoch nicht immer vermeiden, z. B. wenn ein Softwareentwickler im Rahmen einer Wartung bzw. Fehlerbehebung hinzugezogen werden muss. Diese Fälle müssen im Vorhinein geregelt werden, eine Ad hoc Hinzuziehung ohne entsprechende vertragliche Regelung ist nicht statthaft.

Anforderung 83. Kann eine Verarbeitung in Drittländern nicht sicher ausgeschlossen werden, so sind im Vorhinein zwischen Auftraggeber und Auftragnehmer vertragliche Regelungen zu treffen, in welchen Ländern oder nach welchen Kapitel V der DS-GVO genügenden Regeln die Verarbeitung in einem Drittland statthaft ist.

Werden Sozialdaten im Rahmen der Fernwartung verarbeiten, so müssend die Vorgaben von § 80 SGB X befolgt werden. D. h.

- Es handelt sich um Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum,
- ist die Schweiz oder
- es liegt für das Drittland ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vor.

Anforderung 84. Werden im Rahmen der Fernwartung Sozialdaten verarbeitet, so gelten die Anforderungen von § 80 Abs. 2 SGB X.

3.4.6.3 Übermittlungen und Verarbeitung durch verbundene Unternehmen

Im Zusammenhang mit Fernwartung kann es vorkommen, dass der Auftragsverarbeiter personenbezogene Daten verarbeitet, die von einer Konzerngesellschaft innerhalb und außerhalb des Europäischen Wirtschaftsraums ("EWR") verarbeitet werden. Dies kann für die Kontinuität und Verfügbarkeit der Dienste notwendig sein, z. B. das Anfordern von Werksunterstützung zur Problemlösung / Fehlerbehebung oder das Beantworten und Bearbeiten von Fragen und (Sicherheits-)Vorfällen außerhalb der Bürozeiten. Für die Verarbeitung personenbezogener Daten durch Konzerngesellschaften des Auftragnehmers, die außerhalb des EWR in einem Land ohne angemessenes Schutzniveau stattfinden, gelten die Vorgaben von Kapitel V der DS-GVO. Kap. V sieht verschiedene Möglichkeiten vor, wie die Sicherheit der Verarbeitung außerhalb des EWR gewährleistet werden kann, insbesondere

- Datenverarbeitung auf der Grundlage eines Angemessenheitsbeschlusses (Art. 45 DS-GVO)
- Verbindliche interne Datenschutzvorschriften („Binding Corporate Rules, BCR) gemäß Art. 47 DS-GVO)
- Nutzung von durch die EU-Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2DS-GVO erlasse Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DS-GVO).

Grundsätzlich ist bei jeder Verarbeitung außerhalb des EWR zu gewährleisten, dass ein den Vorgaben der DS-GVO genügendes Schutzniveau sowohl der Betroffenenrechte als auch der Sicherheit der Verarbeitung gewährleistet wird.

Anforderung 85. Der Auftragsverarbeiter muss sich (gegebenenfalls) verpflichten, für den Kunden angemessene Unterstützung bei der Beantragung einer Erlaubnis, Genehmigung oder Zustimmung, die möglicherweise nach geltendem Datenschutzrecht für die Umsetzung der Regelungen in dieser Ziffer erforderlich ist, zu leisten.

Bei Verarbeitungen personenbezogener Daten in einem Drittland erfordert es die Transparenz gegenüber der betroffenen Person, dass diese vom Verantwortlichen über den Umstand der Drittstaatenverarbeitung informiert wird. Hierzu bedarf es in der Regel aber Informationen von Auftragsverarbeiter, da häufig dieser die Sicherheit der Verarbeitung adressiert. Dies gilt insbesondere beim Einsatz von BCR.

Anforderung 86. Der Verantwortliche als der für die Verarbeitung Verantwortliche gewährleistet, dass betroffene Personen angemessen über die Möglichkeit der Verarbeitung ihrer personenbezogenen Daten außerhalb des EWR informiert werden. Der Auftragsverarbeiter muss ihm alle dafür benötigten Informationen bereitstellen.

BCR[10] gelten für den Auftragsverarbeiter und seine Konzerngesellschaften und gewährleisten, dass personenbezogene Daten im Sinne von Artikel 47 DSGVO unabhängig vom Ort der Verarbeitung angemessen geschützt sind.

Anforderung 87. Der Auftragsverarbeiter muss sich verpflichten, die Genehmigung der Auftragsverarbeiter BCR durch die zuständigen EU-Behörden während der Laufzeit der Fernwartungsvereinbarung aufrechtzuerhalten und den Verantwortlichen unverzüglich über wesentliche Änderungen an der EU-weiten Genehmigung der BCR zu benachrichtigen.

Anforderung 88. Der Auftragsverarbeiter stellt sicher, dass Übermittlungen an Dritte, die als Unterauftragsverarbeiter agieren, auf der Grundlage rechtlich anerkannter Übertragungsverfahren erfolgen, die im Einklang mit der BCR stehen.

3.5 Umgang mit Testdaten

Die Verwendung von personenbezogenen Daten für Testzwecke sollte vermieden werden. Wenn personenbezogene Informationen für Testzwecke verwendet werden, müssen alle sensiblen Details und Inhalte durch Entfernung oder Veränderung geschützt werden

3.5.1 Zugangssteuerung

Ein Zugriff auf ein Produktivsystem beinhaltet immer auch das Risiko der Beeinträchtigung– ob gewollt oder ungewollt – des Produktivsystems. Daher sollte, wann immer möglich, ein Zugriff auf das Produktivsystem vermieden und stattdessen mit Testumgebungen gearbeitet werden

[10] Siehe auch Art. 47 DS-GVO sowie die WP 256 Rev. 01 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), 265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848) und 257 Rev. 01(https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110), die vom EDPB angenommen wurden (siehe https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de).

Anforderung 89. **Die Fernwartung erfolgt, wenn möglich in Testumgebungen; der Zugriff auf das Produktivsystem sollte nur gewählt werden, wenn ein Wartungsziel anders nicht erreicht werden kann.**

Anforderung 90. **Die Zugangssteuerungsverfahren, die für den Einsatz der Produktivsysteme gelten, gelten auch für die Testsysteme.**

3.5.2 Berechtigung

Anforderung 91. **Es ist jedes Mal eine separate Berechtigung erforderlich, wenn Informationen aus einem Produktivsystem in eine Testumgebung kopiert werden.**

3.5.3 Löschung

Anforderung 92. **Nach Abschluss der Überprüfung werden die Betriebsinformationen aus der Testumgebung gelöscht.**

3.5.4 Protokollierung

Anforderung 93. **Das Kopieren und die Verwendung von Informationen aus Produktivsystemen werden protokolliert.**

4 Glossar

Auftraggeber	Siehe Verantwortlicher
Auftragnehmer	Siehe Auftragsverarbeiter
Auftragsverarbeiter	Die natürliche oder juristische Person, welche sich zur Erbringung der Fernwartungstätigkeit verpflichtete. – Im Rahmen von Verträgen zur Auftragsverarbeitung ist es der Auftragsverarbeiter – Bei einer „Gemeinsamen Verarbeitung“ ist es entweder einer der Verantwortlichen oder ein separat beauftragter Auftragsverarbeiter – Bei einer eigenständig durchgeführten Fernwartung ist es die interne Abteilung, welche die Fernwartung leistet
Authentisierung	Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators (Quelle: DIN EN ISO 22600-1)
Authentisierung, starke	Authentisierung mittels kryptographisch abgeleiteter multifaktorieller Identitätsnachweise (Quelle: DIN EN ISO 22600-1)
Drittland	Ein Land, welches sich außerhalb der EU/EWR befindet.
Fernwartung	Räumlich getrennter Zugriff auf IT-Systeme oder andere Produkte zu Wartungs-, Reparatur- und anderen Unterstützungszwecken unter Nutzung der Möglichkeiten der Informations- und Kommunikationstechnik (IKT)
Fernwartungssoftware	Jede Software, welche eine Fernwartung ermöglicht
Identifizierung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen (Quelle: ISO/IEC 2382-8])
Integrität	Eigenschaft, die bedingt, dass die Information in keiner Weise, weder absichtlich noch unabsichtlich, geändert wird (Quelle: DIN EN ISO 22600-2)
Nicht-Abstreitbarkeit	Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Einheiten an dem Ereignis zu entscheiden (Quelle. DIN ISO/IEC 27000)
Rolle	Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen (Quelle: DIN EN ISO 22600-1)
Session	Synonym für Sitzung
Sitzung	Ein konkreter Fernwartungsvorgang
Unterauftragnehmer	Vom Auftragnehmer beauftragter Leistungserbringer, dessen Dienstleistung und/oder Werk der Auftragnehmer zur Erbringung der in diesem Vertrag beschriebenen Leistungen gegenüber dem Auftraggeber benötigt

Unternehmen	Der Begriff wird in dieser Ausarbeitung dergestalt verwendet, wenn eine juristische oder natürliche Person sich unternehmerisch planend und entscheidend betätigt.
Verantwortlicher	Die natürliche oder juristische Person, welche die Software oder das Produkt betreibt, welches per Fernwartung betreut werden soll. – Im Rahmen von Verträgen zur Auftragsverarbeitung ist es der Verantwortlich – Bei einer „Gemeinsamen Verarbeitung“ ist es mindestens einer der Verantwortlichen – Bei einer eigenständig durchgeführten Fernwartung ist es der Arbeitgeber
Verfügbarkeit	Eigenschaft, auf Nachfrage einer berechtigten Entität zugreifbar und verwendbar zu sein (Quelle: SO/IEC 27000)
Verlässlichkeit	Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen (Quelle. DIN ISO/IEC 27000)
Vertraulichkeit	Eigenschaft, dass Informationen gegenüber unberechtigten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder an diese weitergegeben werden (Quelle: ISO 7498-2)
Weisung/Anweisung	Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch einen Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).
Zugriffskontrolle	Sicherung, dass ausschließlich autorisierte Entitäten auf zugriffsberechtigte Weise Zugang zu Ressourcen eines Datenverarbeitungssystems haben (Quelle: ISO/IEC 2382-8)
Zugriffssteuerung	Mittel zur Sicherstellung, dass nur autorisierte Entitäten in entsprechend autorisierter Weise Zugriff auf die Ressourcen eines Datenverarbeitungssystems nehmen können (Quelle: ISO/IEC 2382-8)
Zurechenbarkeit	Eigenschaft, durch die sichergestellt wird, dass die Aktionen einer Entität eindeutig auf diese zurückgeführt werden können (Quelle: ISO 7498-2)

5 Abkürzungsverzeichnis

AdVermiG	Gesetz über die Vermittlung der Annahme als Kind und über das Verbot der Vermittlung von Ersatzmüttern (Adoptionsvermittlungsgesetz)
Art.	Artikel
Artt.	Artikel (Mehrzahl)
ASLR	Address Space Layout Randomization
BetrVG	Betriebsverfassungsgesetz
BIOS	basic input/output system
BPersVG	Bundespersonalvertretungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
conductDEP	Data Execution Prevention
DMZ	Demilitarisierte Zone
DS-GVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
EFI	Extensible Firmware Interface (am bekanntesten: Unified EFI, kurz UEFI)
ErwGr.	Erwägungsgrund
GDD	Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz für die Bundesrepublik Deutschland
IP	Internet Protocol
MAC	Message Authentication Code
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte.
PSK	Pre-Shared Key
SFTP	SSH File Transfer Protocol
SGB	Sozialgesetzbuch
SSH	Secure Shell
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TR	Technische Richtlinie

Anhang 1. Hilfestellung für Technische Maßnahmen

Anhang 1 enthält die Verweise auf weitere Hilfsmittel. Hier werden zunächst Beispiele aus deutschen Normen zitiert. Der Bezug auf internationale Normen in der Umsetzung ist genauso möglich.

- 3.1.1 Definition der zu schützenden Informationen
  Eine Hilfestellung zur Definition der zu schützenden Informationen/Daten findet der Verantwortliche z.B. in Kap. 8.2 des BSI-Standard 200-2[11]
- 3.1.4 Rechte des Verantwortlichen
  Eine Hilfestellung zu findet der Verantwortliche in Kap. 10.1 BSI 200-2[11]
- 3.1.6 Informationsfluss und Meldewege bei Datenpannen sowie vertragliche Regelungen bzgl. unbefugter Offenbarung
  Eine Hilfestellung findet der Verantwortliche in Kap. 5.2 BSI 200-2[11]

[11] BSI-Standard 200-2 - IT-Grundschutz-Methodik. [Online, zitiert am 2021-08--30]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html bzw. pdf-Datei unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html?nn=128640

Anhang 2. Wer muss welche Anforderungen erfüllen?

Anhang 2.1. Anforderungen, die seitens des Verantwortlichen erfüllt werden müssen

Die nachfolgend aufgelisteten Anforderungen adressieren in erster Linie den oder die Verantwortlichen:

- Anforderung 1
- Anforderung 4
- Anforderung 5
- Anforderung 9
- Anforderung 16
- Anforderung 18
- Anforderung 19
- Anforderung 21
- Anforderung 27
- Anforderung 35
- Anforderung 37
- Anforderung 38
- Anforderung 39
- Anforderung 40
- Anforderung 41
- Anforderung 44
- Anforderung 45
- Anforderung 46
- Anforderung 47
- Anforderung 49
- Anforderung 50
- Anforderung 51
- Anforderung 52
- Anforderung 53
- Anforderung 54
- Anforderung 55
- Anforderung 56
- Anforderung 57
- Anforderung 58
- Anforderung 59
- Anforderung 60
- Anforderung 61
- Anforderung 62
- Anforderung 63
- Anforderung 64
- Anforderung 65
- Anforderung 66
- Anforderung 67
- Anforderung 68
- Anforderung 69

- Anforderung 72
- Anforderung 73
- Anforderung 74
- Anforderung 75
- Anforderung 76
- Anforderung 77
- Anforderung 78
- Anforderung 79
- Anforderung 80
- Anforderung 86
- Anforderung 93

Anhang 2.2. Anforderungen, die seitens des Auftragsverarbeiters erfüllt werden müssen

Die nachfolgend aufgelisteten Anforderungen adressieren in erster Linie den oder die Auftragsverarbeiter:

- Anforderung 3
- Anforderung 4
- Anforderung 5
- Anforderung 6
- Anforderung 7
- Anforderung 8
- Anforderung 10
- Anforderung 11
- Anforderung 13
- Anforderung 14
- Anforderung 15
- Anforderung 20
- Anforderung 27
- Anforderung 35
- Anforderung 36
- Anforderung 37
- Anforderung 38
- Anforderung 44
- Anforderung 45
- Anforderung 47
- Anforderung 49
- Anforderung 50
- Anforderung 51
- Anforderung 52
- Anforderung 53
- Anforderung 54
- Anforderung 55
- Anforderung 56
- Anforderung 57
- Anforderung 58

- Anforderung 59
- Anforderung 60
- Anforderung 61
- Anforderung 69
- Anforderung 72
- Anforderung 74
- Anforderung 75
- Anforderung 76
- Anforderung 77
- Anforderung 79
- Anforderung 80
- Anforderung 85
- Anforderung 87
- Anforderung 88

Anhang 2.3. Anforderungen, die sowohl Verantwortlicher als auch Auftragsverarbeiter adressieren

Die nachfolgend aufgestellten Anforderungen können in der Regel nicht von einem Vertragspartner – sei es Verantwortlicher oder Auftragsverarbeiter - alleine durchgeführt werden, weil z.B. die Kommunikationsverbindung von beiden Vertragsparteien abgesprochen werden muss oder weil die Partner ein spezielles Vorgehen vereinbaren müssen.

Grundsätzlich sollte bei jeder Fernwartung darauf hingewirkt werden, die nachfolgend genannten Anforderungen mit dem oder den jeweiligen Vertragspartnern umzusetzen:

- Anforderung 2
- Anforderung 12
- Anforderung 17
- Anforderung 22
- Anforderung 23
- Anforderung 24
- Anforderung 25
- Anforderung 26
- Anforderung 28
- Anforderung 29
- Anforderung 30
- Anforderung 31
- Anforderung 32
- Anforderung 33
- Anforderung 34
- Anforderung 42
- Anforderung 43
- Anforderung 48
- Anforderung 70
- Anforderung 71
- Anforderung 81
- Anforderung 82

- Anforderung 83
- Anforderung 84
- Anforderung 89
- Anforderung 90
- Anforderung 91
- Anforderung 92