CIRSmedical Anästhesiologie

Critical- Incident-Reporting-System
für Anästhesie, Intensivtherapie, Notfallmedizin und Schmerztherapie

Startpaket

(Version 11-2022)

Informationen
zur Teilnahme am Incident Reporting System

CIRSmedical Anästhesiologie

von BDA/DGAI und BÄK

Dokument 1:	**Checkliste CIRS-AINS Teilnahme**
Dokument 2:	**Rahmenvereinbarung**
Dokument 3:	**Fragebogen Einrichtung CIRS-AINS**
Dokument 4:	**Mitarbeiter-Information**
Dokument 5:	**CIRS-AINS Beauftragte**
Dokument 6:	**Datenschutz, Erklärung und Merkblatt**
Dokument 7:	**Aussageverweigerungsrecht**
Dokument 8:	**Infoblatt CIRS-AINS Schulung**
Dokument 9:	**Gebührenübersicht**
Dokument 10:	**Formular Änderung CIRS-AINS Beauftragte**
Dokument 11:	**Konformitätserklärung/Teilnahmebestätigung**

www.CIRS-AINS.de

CIRSmedical Anästhesiologie

Checkliste CIRS-AINS Teilnahme 

1. Informieren Sie die Leitungsebene und je nach Institution die Rechtsabteilung, die Mitarbeitervertretung/Personalrat/Betriebsrat und Datenschutzbeauftragte über die geplante Einführung von CIRS-AINS. ☐
2. Lesen und unterzeichnen Sie die Rahmenvereinbarung **(Dokument 2).** Neben der externen Anonymisierung (Basispaket) können Sie zusätzlich eine externe interdisziplinäre Analyse Ihrer Fallberichte inklusive fallbezogenem Feedback durchführen lassen (Analysepaket). Nähere Informationen hierzu finden Sie im **Dokument 3**. Eine Übersicht über die anfallenden Gebühren finden Sie in **Dokument 9.** ☐
3. Bitte füllen Sie den Fragebogen für die Einrichtung von CIRS-AINS aus **(Dokument 3).** ☐
4. Informieren Sie das Personal im Sinne des „internen Sanktionsschutzes“: Höchste Priorität haben Vertraulichkeit und Interesse an Verbesserungen zur Erhöhung der Patientensicherheit, es geht nicht um die Identifikation von „Schuldigen“. Geben Sie allen Mitarbeitenden die schriftliche Zusicherung, dass keine negativen personellen Konsequenzen aus Berichten an CIRS-AINS zu befürchten sind. Dafür können Sie die im Startpaket enthaltene Vorlage verwenden **(Dokument 4).** ☐
5. Benennen Sie je nach Institutsgröße mehrere CIRS-AINS Beauftragte je Berufsgruppe (Ärzte und Pflegekräfte) **(Dokument 5).** Versuchen Sie Ihre Abteilung entsprechend abzudecken (OP, Intensiv etc). ☐
6. Alle CIRS-AINS-Beauftragte müssen einzeln im Sinne der DSGVO gegenüber dem Betreiber schriftlich zur Verschwiegenheit verpflichtet werden (Grundsatz hierfür ist: DSGVO, Art. 32, Sicherheit der Verarbeitung) **(Dokument 6)** und über Ihr Aussageverweigerungsrecht informiert werden **(Dokument 7).** ☐
7. Bei Buchung des Basispaketes sollten die CIRS-AINS Beauftragten und evtl. weitere ärztliche und pflegerische Mitarbeiter an einer CIRS-AINS Basisschulung teilnehmen **(Dokument 8).** Die Schulung ist jederzeit online möglich. Generell wird die Teilnahme an einer Schulung empfohlen. ☐
8. **Senden Sie die Dokumente Nr. 2-6 im Original unterzeichnet an untenstehende Adresse**. Bitte bewahren Sie Kopien für Ihre Unterlagen auf. ☐
9. Nach Eingang aller Dokumente wird die CIRS-AINS Startseite Ihrer Institution eingerichtet. Über diese Startseite wird Ihre Einrichtung mit der CIRSmedical Software verlinkt. Nach erfolgter Freischaltung Ihres Zugangs zu CIRS-AINS werden Sie unverzüglich schriftlich informiert. Die Abrechnung der anfallenden Gebühren durch die BDA/DGAI beginnt am 1. des darauffolgenden Monats.

BDA/DGAI Geschäftsstelle
CIRS-AINS
Neuwieder Str. 9
90411 Nürnberg
Tel.: 0911 – 933 78 0
info@cirs-ains.de

CIRSmedical Anästhesiologie

Rahmenvereinbarung

zur Nutzung und Teilnahme am Incident Reporting System CIRS-AINS von BDA/DGAI und BÄK

Hintergrund

In den kommenden Monaten wird in Ihrer Institution das Critical-Incident-Reporting-System CIRSmedical Anästhesiologie (CIRS-AINS) von BDA/DGAI und Bundessärztekammer (BÄK) eingeführt. Dieses internetbasierte System dient der anonymen und sanktionsfreien Erfassung und Verbreitung von sicherheitsrelevanten Ereignissen in Klinik und Praxis und wird von BDA und DGAI bundesweit für ihre Mitglieder zur Verfügung gestellt.

Als „sicherheitsrelevante Ereignisse“ werden alle Abweichungen vom regelhaften Verlauf, Fehler, kritische Ereignisse und Beinahe-Unfälle bezeichnet, welche die Patientensicherheit gefährdet haben oder haben könnten. Es sollen aber auch positive Lösungen für kritische Situationen gemeldet werden, da auch Tipps, Tricks und Anregungen für eine kritische Situation sicherheitsrelevant sind. Bitte berichten Sie vor allem auch Ereignisse, die rechtzeitig aufgedeckt wurden, die aber jederzeit so wieder auftreten könnten. Jedem katastrophalen Verlauf gehen ähnliche Fälle voraus, die glimpflich ausgehen. Wer diese aufdeckt und bearbeitet, vermeidet den folgeschweren Fehler.

CIRSmedical Anästhesiologie kann so – als Bestandteil eines umfassenden Risikomanagements – zur Transparenz der Arbeit beitragen. Es liefert wertvolle Hinweise auf Risiken, die bislang nicht entdeckt wurden. Die CIRS-Eingaben sind unschätzbare Beiträge der Mitarbeiter. Deshalb werden alle Mitarbeiter gebeten, diese wichtige Neuerung zu unterstützen. Die Eingaben sind anonym. Sie werden bei der Bearbeitung im ersten Schritt darauf überprüft, ob sie durch Detailangaben die Anonymität des Berichtenden gefährden. Solche Angaben werden zurückgehalten.

Details zum System finden Sie im Internet unter: https://www.cirs-ains.de/cirs-ains/cirs-ains-informationen.html oder können der Publikation „Fehlermanagement mit CIRS“ https://www.cirs-ains.de/files/CIRS_Fehlermanagement.pdf entnommen werden. Die Grundkosten für die Software, die Pflege und den Betrieb des Systems, sowie dessen kontinuierliche Weiterentwicklung werden dabei von BDA/DGAI übernommen.

Lediglich für die fallbezogenen Leistungen (Anonymisierung und das optionale Analyse-Modul) werden Gebühren erhoben. Das optionale Fallanalyse- und Feedback-Modul beinhaltet die interdisziplinäre professionelle Analyse von Berichten und das fallbezogene Feedback inklusive Verbesserungsmaßnahmen an die betreffende Institution.

Wird das CIRS-AINS Tool entgegen seiner Bestimmung gebraucht, wird also z. B. einmal die Anonymitätszusicherung verletzt, so kann der Schaden sehr leicht über die lokale Institution hinaus gehen und sich möglicherweise unwiderruflich negativ auf das gesamte Incident Reporting in Deutschland auswirken. Dies könnte bei den Nutzern zu einem Vertrauensverlust bezüglich des Systems führen, was u. U. zur Folge hätte, dass keine Berichte mehr eingetragen werden würden. Aus diesem Grunde ist es essentiell, dass sich die beteiligten Institutionen bzw. die CIRS-AINS Beauftragten vor Ort der Bedeutung und Verantwortung ihrer Arbeit bewusst sind. Für den Erfolg von CIRSmedical Anästhesiologie in Deutschland und damit für die Patientensicherheit ist die sachgerechte Nutzung des Tools entscheidend.

Um die Sicherheit für die Nutzer und die Effektivität des Systems zu optimieren, wird mit den Beteiligten die folgende Rahmenvereinbarung schriftlich geschlossen.

Rahmenvereinbarung

für die Nutzung von CIRSmedical Anästhesiologie

Die hier genannten Rahmenbedingungen für die Nutzung von CIRSmedical Anästhesiologie (CIRS-AINS) von BDA/DGAI und BÄK haben verpflichtenden Charakter und werden schriftlich vereinbart. Nichtbeachtung kann zum Ausschluss von der Teilnahme führen.

1) Vor der Einführung informiert die Leitung der Abteilung die Mitarbeitenden über die Einführung von CIRS-AINS. Außerdem sollte die Einführung mit der Rechtsabteilung des Hauses sowie entsprechenden Personalvertretungen (**Personal- oder Betriebsrat, Mitarbeitervertretung)** abgestimmt werden. Analog wird die **Information und Zustimmung der Krankenhausleitung** empfohlen. Die Abteilungsleitung sichert den Mitarbeitern die Sanktionsfreiheit bei der Teilnahme an CIRS-AINS zu (Dokument 4). Es wird empfohlen, diese Zusicherung der Sanktionsfreiheit auch von der Krankenhausleitung unterschreiben zu lassen. Die Zustimmung der Personalvertretung sollte durch die zugesicherte Sanktionsfreiheit und Anonymität des CIRS-AINS Systems im Allgemeinen kein Problem darstellen. **Datenschutzbeauftragte** sollten ebenso eingebunden werden.

Zur Grundinformation gehört auch die „Verpflichtung zur wahrheitsgemäßen Meldung“ (s. Dokument 4). Dieser Wahrheitsgrundsatz ist insbesondere bei Meldungen im Zusammenhang mit Medizinprodukten oder Arzneimitteln zu beachten (Thema: Schadensersatz durch entsprechende Firmen).

2) Die **Krankenhausleitung sichert ihren Mitarbeitern die Vertraulichkeit** der gemeldeten Daten zu. Jeder Mitarbeiter kann darauf vertrauen, dass die in CIRS-AINS eingegebenen Berichte anonym und sanktionsfrei bleiben. Die Geschäftsführung bestätigt ausdrücklich, dass kein Mitarbeiter, der Eingaben ins CIRS macht, Sanktionen aufgrund seines Berichts oder der berichteten Ereignisse zu befürchten hat. Sie bestätigt, dass keinerlei Anstrengungen unternommen werden, die Anonymität der CIRS-Berichtenden aufzudecken. Sie garantiert den Mitarbeitern, die die CIRS-Eingaben bearbeiten, dass sie keine vertraulichen Details aus den Eingaben preisgeben müssen. Der Sinn von CIRS-AINS ist die Erhöhung der Patientensicherheit. Es geht nicht darum „Schuldige“ zu finden. Ein Formular zur empfohlenen Aushändigung an alle Mitarbeiter hierfür liegt bei (Dokument 4). Idealerweise wird dieses von allen Beteiligten (z.B. ärztliche und kaufmännische Geschäftsleitung und PDL) unterzeichnet. Bitte senden Sie eine Kopie dieses unterzeichneten Schreibens an BDA/DGAI.

3) Die Leitungsebene benennt mindestens einen ärztlichen **CIRS-AINS Beauftragten**. Es wird allerdings empfohlen für alle Berufsgruppen (Ärzte, vor allem aber auch Pflegekräfte) jeweils einen Beauftragten zu benennen und an die Anzahl der Abteilungsgröße sinnvoll anzupassen. Ideal erscheint für jeden größeren Bereich ärztliche und pflegerische Beauftragte zu benennen (z. B. Intensivstation und OP). Diese werden schriftlich mit Kontaktdaten (Telefon, Email, Anschrift) an BDA/DGAI gemeldet (s. Dokument 5).

Aufgaben der CIRS-AINS Beauftragten sind:

- Koordination der aus den Fallberichten (und ggf. der Analyse) gewonnenen Erkenntnisse und Verbesserungsvorschläge mit ihren abzuleitenden Konsequenzen (Letzteres in Absprache und mit Unterstützung durch die Klinikleitung und ein evtl. vorhandenes Risikomanagement).
- Monitoring der umzusetzenden/umgesetzten Maßnahmen, Rückmeldung und Information an CIRS-AINS.
- Klärung von Problemen vor Ort und Ansprechpartner für CIRS-AINS.

Die CIRS-AINS Beauftragten sollten für ihre Aufgaben in ausreichendem Umfang freigestellt werden.

Die CIRS-AINS Beauftragten werden **schriftlich gemäß Art. 28 Abs. 3 S. 2 Lit. b DS-GVO auf Verschwiegenheit verpflichtet** (s. Dokument 6). Dies soll die hohe Bedeutung des Datenschutzes, sowie der Schweigepflicht sowohl nach intern und als auch extern in Bezug auf meldende und/oder betroffene Personen (Mitarbeiter, Patienten) gewährleisten und unterstreichen. Erst nach Vorliegen dieser Verpflichtungen kann das System für die jeweilige Institution in Betrieb gehen.

4) Um die optimale Nutzung von CRIS-AINS zu gewährleisten, wird eine entsprechende Expertise der Verantwortlichen aus den beteiligten Institutionen empfohlen. Alle CIRS-AINS Beauftragten sollten an der **Basisschulung im Umgang mit CIRS-AINS** teilnehmen. Inhalt und Ziel der Schulung sind im Wesentlichen die Nutzung und Sicherheit von CIRS-AINS, sowie die Darstellung möglicher Maßnahmen zur Analyse und zum Feedback eingegangener Meldungen.

Im Rahmen des **e-Learning-Portals** von BDA und DGAI ist die Basisschulung in Form einer Onlineschulung verfügbar.

5) Ablauf und externe Anonymisierung der Fälle durch CIRS-AINS: Die Berichte werden über eine SSL-verschlüsselte Internet-Datenleitung auf den Hochsicherheitsserver des Universitätsklinkums Basel übertragen. Jegliche weitere Bearbeitung erfolgt auf diesem Server. Die eingegangenen Berichte der teilnehmenden Institutionen werden vor ihrer Freigabe von erfahrenen Experten innerhalb kurzer Zeit anonymisiert. Jede Anonymisierung wird von zwei Anonymisierer unabhängig voneinander vorgenommen (4-Augen-Prinzip), die Originalberichte anschließend gelöscht.
Da keine personen- oder ortsbezogenen Daten (z.B. IP-Adressen) mit dem Bericht gespeichert werden, ist eine Zuordnung oder Nachverfolgung zu einzelnen Einrichtungen oder Personen nicht möglich. Erst nach abgeschlossener Anonymisierung wird der Bericht sowohl in Ihrer einrichtungsinternen Untergruppe als auch im öffentlichen Bereich über die Homepage des Netzwerkes lesbar.

Die zentrale Anonymisierung durch CIRS-AINS bietet vor allem **deutliche juristische Vorteile (s. auch bei 6):**

i) Durch die zentrale Speicherung der Berichte auf einer zentralen Datenbank innerhalb eines Hochsicherheitsservers außerhalb Deutschlands besteht prinzipiell ein hoher Schutz vor Beschlagnahme.

ii) Aufgrund presserechtlicher Bestimmungen besteht zudem ein Zeugnisverweigerungsrecht auf Seiten der Betreiber von CIRS-AINS. Dies ist ein immenser Vorteil des zentralen CIRS-AINS Systems, insbesondere im Zusammenhang mit der externen Anonymisierung.

iii) Durch die komplett externe Abwicklung können lokal keine Daten eingesehen oder beschlagnahmt werden.

Für die Einrichtung von CIRSmedical Anästhesiologie wird jeder Einrichtung eine eigene Startseite zur Verfügung gestellt. Über eine feste IP-Adresse wird diese Startseite mit der Software CIRSmedical verlinkt. Dieses ermöglicht, dass nur Computer die zu diesem IP-Adressenbereich gehören auf die Startseite zugreifen können. Somit ist das Fehlerberichts- und Lernsystem von außerhalb der Einrichtung nicht zugänglich und die anonymisierten Fälle der eigenen Einrichtung können selektiv eingesehen werden. So übernimmt **CIRS-AINS einerseits die Funktion eines lokalen Incident Reporting Systems**, mit dem Vorteil der zentralen Datenspeicherung und externen Anonymisierung. Andererseits sind die Fälle im Rahmen des bundesweiten Netzwerkes für alle lesbar, was die Effektivität und Verbreitung der einzelnen Ereignisse verbessert.
Für die fallbezogene Anonymisierung fallen geringe Kosten an, welche in der Gebührenübersicht dargestellt sind (**Gebührenübersicht s. Dokument 9**). Die Nutzung dieser zusätzlichen Option kann in **Dokument 2** vereinbart werden.

6) Die Daten sind im zentralen System CIRS-AINS mit hoher Sicherheit für juristische Belange nach Presserecht geschützt (Beschlagnahmeeinschränkung etc, s. Dokument 7). Durch die Speicherung im zentralen Informationsdienst von CIRS-AINS besteht ein Zeugnisverweigerungsrecht, welches sich sowohl auf die Daten, als auch die CIRS-AINS Mitarbeiter (z.B. für Anonymisierer, CIRS-Beauftragte bei Ihnen vor Ort) erstreckt. Dies ist ein enormer Vorteil im Vergleich zu allen lokalen Systemen, deren Daten prinzipiell jederzeit von entsprechenden Institutionen beschlagnahmt und beteiligte Personen verhört werden können.

7) Im optional erhältlichen **Analyse- und Feedback-Modul (kostenpflichtig buchbar)** werden die Berichte der teilnehmenden Institution durch ein interdisziplinäres Expertenteam auf Ursachen und begleitende Faktoren untersucht. Das Expertenteam leitet aus den Analyseergebnissen gegebenenfalls ein einzelfallbezogenes Feedback mit Vorschlägen zur systematischen Verbesserung ab. Diese neutralen, externen Ergebnisse und Vorschläge werden dem Fallbericht angefügt und lesbar geschaltet. Die Aufgabe der CIRS-AINS Beauftragten liegt dann darin, die empfohlenen Maßnahmen zu sichten, auf Durchführbarkeit zu prüfen und die Implementierung in der Institution zu koordinieren.
Sie erhalten durch diese zusätzliche Option für jeden Fall eine neutrale externe, interdisziplinäre Analyse Ihrer kritischen Ereignisse. Mit diesem „Blick über den Tellerrand“ und über institutionseigene Gewohnheiten hinaus, können Sie Ihre Maßnahmen zur Verbesserung gezielter durchführen und auch unabhängig, zum Beispiel der Verwaltung gegenüber, begründen.

Wenn Ihre CIRS-AINS Beauftragten den Stand der Umsetzung etwaiger Maßnahmen an Ihre Institution und an CIRS-AINS rückmelden, kann sich der Kreis von der Eingabe des Berichts hin zur Umsetzung und Verbreitung durchgeführter Maßnahmen sinnvoll schließen.
Die Nutzung des Analysemoduls ist für jede Institution optional und kostenpflichtig. Die Gebühren werden ebenso wie die externe Anonymisierung in Abhängigkeit von der Anzahl der ärztlichen Mitarbeiter einer Institution berechnet (**Gebührenübersicht s. Dokument 9**). Die Nutzung dieser zusätzlichen Option kann mit BDA/DGAI vereinbart werden (**Dokument 2**).

8) CIRS-AINS **stellt in keiner Weise einen Ersatz für anderweitig vorgeschriebene interne oder externe Meldungen von Zwischenfällen dar.** Haftungsrechtlich oder gesetzlich vorgeschriebene Meldungen (z.B. Arzneimittelnebenwirkungen, MPG-Meldungen an das BfArM etc) werden durch CIRS-AINS nicht ersetzt, ebenso wenig die Information des Patienten oder der Angehörigen. Durch die Anonymität der Meldungen kann ein Incident Reporting System wie CIRS-AINS bzw. dessen Beauftragte diese Funktion nicht leisten. Zur Klärung straf- und zivilrechtlich relevanter Vorkommnisse kann CIRS-AINS darüber hinaus aufgrund der Anonymisierung der Fälle nicht herangezogen werden.

9) Haftungsausschluss: Schutz- und Verbesserungsmaßnahmen müssen immer lokal vor Ort getroffen werden. CIRS-AINS kann aufgrund der Freiwilligkeit und Anonymisierung keine Gewähr für wichtige Warn- oder Verbesserungsmeldungen übernehmen. Die Meldungen in CIRS-AINS stammen von anonymen Meldern, die im Prinzip Mitarbeiter an jeder beliebigen Institution sein können. Damit kann für die Verbindlichkeit der Aussagen in CIRS-AINS keine Gewähr übernommen werden. Alle genannten Empfehlungen müssen im Einzelfall kritisch bewertet und von kompetentem Fachpersonal auf Anwendbarkeit, Sinnhaftigkeit und Sicherheit überprüft werden. Eine Haftung für direkte oder indirekte Schäden (Rufschädigung etc), die sich aus Meldungen an CIRS-AINS oder den Betrieb von CIRS-AINS ergeben, auch solche durch unzureichende Anonymisierung, ist explizit und umfassend ausgeschlossen, sofern nicht grobe Fahrlässigkeit oder Vorsatz auf Seiten von CIRS-AINS nachgewiesen werden kann.

Vorstehender Haftungsausschluss gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer fahrlässigen Pflichtverletzung beruhen, sowie für sonstige Schäden, die auf einer grob fahrlässigen Pflichtverletzung oder Vorsatz beruhen.

10) Nutzungsumfang: Die beiden Verbände BDA und DGAI verfügen über das ausschließliche Nutzungsrecht an den an CIRS-AINS übermittelten Daten.
Die Nutzer sind berechtigt, die Inhalte zu privaten Zwecken zu nutzen und in den Arbeitsspeicher ihres Rechners zu kopieren. Die Nutzer sind zur Herstellung von Vervielfältigungsstücken (zum Beispiel Ausdruck von Web-Seiten oder eines Beitrages) nur zu privaten Zwecken beziehungsweise zu eigenen Informationszwecken berechtigt. Die Nutzer dürfen darüber hinaus die abgerufenen Beiträge ausschließlich zum eigenen Gebrauch nutzen. Diese Berechtigungen gelten nur, wenn Schutzvermerke (Copyright-Vermerke und ähnliches) sowie Wiedergaben von Marken und Namen in den Vervielfältigungsstücken unverändert erhalten bleiben.
Für alle weiteren Nutzungen (unter anderem - aber nicht ausschließlich - für die Vervielfältigung zu gewerblichen Zwecken einschließlich der Archivierung, für die Überlassung an oder Verarbeitung durch Dritte für eigene oder fremde Zwecke oder zur öffentlichen Wiedergabe sowie für die Übersetzung, Bearbeitung, das Arrangement oder andere Umarbeitungen) bedarf es der vorherigen schriftlichen Zustimmung von BDA und DGAI.

11) Die **Teilnahme an CIRS-AINS ist freiwillig** und kann mit dreimonatiger Kündigungsfrist zum Quartalsende jederzeit von beiden Seiten (BDA/DGAI und Nutzer) beendet werden.

CIRS-AINS ist keine Beschwerdeplattform

In den vergangenen Jahren sind eine ganze Reihe an Meldungen bei CIRS-AINS eingegangen, die nicht die Kriterien eines CIRS-Berichtes erfüllen. CIRS-Systeme haben die Zielsetzung, unerwartete Ereignisse mit Sicherheitsrelevanz zu erfassen, diese zu analysieren und – wo sinnvoll – konstruktive Maßnahmen daraus abzuleiten.

Viele der Meldungen thematisieren jedoch bekannte und alltägliche Probleme und Konflikte. So ist beispielsweise die im Gesundheitswesen allgegenwärtige Personalknappheit zwar sicherheitsrelevant, jedoch kann eine Meldung in CIRS-AINS im Sinne einer Überlastungsanzeige der Mitarbeiterinnen und Mitarbeiter keinerlei konstruktive Veränderung bewirken. Des Weiteren erfüllen auch Berichte, die über nicht nachvollziehbare Entscheidungen einzelner Personen, über ungenügende Teamarbeit oder fehlende Kommunikation berichten, nicht die Kriterien eines CIRS-Berichtes. Denn die einzig sinnvolle und konstruktive Konsequenz aus diesen Ereignissen ist das Gespräch aller Beteiligten miteinander, welches klären und gegenseitiges Verständnis herbeiführen soll. Eine anonyme Eingabe in ein CIRS-Programm hilft hier nicht weiter, sondern birgt im Gegenteil die Gefahr, dass die Meldung als Beschwerde oder als öffentliche Bloßstellung einer Kollegin/eines Kollegen interpretiert wird: die Beschwerde einer Berufsgruppe über eine andere oder die Diskreditierung einzelner Personen.

Ein solches Vorgehen ist im Hinblick auf die Akzeptanz und Vertrauenswürdigkeit eines CIRS-Systems und damit eben auch für unser gemeinsames Anliegen der Stärkung der Patientensicherheit kontraproduktiv.

Wir bitten daher um Verständnis, dass wir uns vorbehalten, zukünftig Fallberichte mit Systemanklagen, Anschwärzen von Kollegen, Hörensagen, Interpretationen bzw. rein sozialen und emotionalen Konflikten weder weiter zu bearbeiteten noch zu veröffentlichen.

Ihr CIRS-AINS Team BDA/DGA

Ich habe die 11 Punkte der CIRS-AINS Rahmenvereinbarung zur Kenntnis genommen und versichere gegenüber BDA/DGAI als Betreiber die Umsetzung und Einhaltung dieser Rahmenbedingungen.

Anzahl der ärztlichen Mitarbeiter/innen der teilnehmenden Abteilung: ☐

☐ Basispaket (gebührenpflichtig):
Anonymisierung und Freigabe der Berichte und Nutzerkommentare durch die Arbeitsgruppe aus BDA-Rechtsabteilung, erfahrenen Anästhesiologen mit langjähriger CIRS-Erfahrung und Experten der Arbeitskreise BDA/DGAI.
Analyse und Feedback der Berichte und Nutzerkommentare durch die eigene CIRS-Analysegruppe Ihres Krankenhauses.

☐ Analysepaket (gebührenpflichtig):
Anonymisierung, Freigabe, Analyse und Feedback der Berichte und Nutzerkommentare durch die Arbeitsgruppe aus BDA-Rechtsabteilung, erfahrene Anästhesiologen mit langjähriger CIRS-Erfahrung und Experten der Arbeitskreise BDA/DGAI.

Die Gebühren werden in Abhängigkeit der Anzahl der ärztlichen Mitarbeiter Ihrer Institution berechnet (Gebührenübersicht s. Dokument 9). Hinweis: Die Anzahl der ärztlichen Mitarbeiter dient dabei nur als Kennzahl, selbstverständlich ist die Beteiligung aller Mitarbeiter (Pflegekräfte, MTA, Technik) damit eingeschlossen.

Der anfallende Betrag wird einmal pro Halbjahr über den BDA in Rechnung gestellt und kann aufwandsbezogen alle 6 Monate neu angepasst werden. Die Vereinbarung kann von beiden Seiten mit dreimonatiger Kündigungsfrist zu jedem Quartalsende beendet werden.

Einwilligung zur Weitergabe von personenbezogenen Daten:
Zum Zweck der technischen Einrichtung und des technischen Supports eines CIRS als Untergruppe des CIRS-AINS bin ich mit der Weiterleitung meiner Daten/Informationen an die Bundesärztekammer (BÄK) einverstanden. Diese Daten werden dort selbstverständlich genauso vertraulich behandelt wie beim BDA und der DGAI.

Ich willige ein, dass die BÄK den BDA stets über die wesentlichen technischen Inhalte zur eingerichteten Untergruppe unterrichtet: ☐ ja ☐ nein

Meine Einwilligung kann ich jederzeit mit Wirkung für die Zukunft widerrufen bei:

Bundesärztekammer (BÄK)
Frau A. Sanguino H.
Herbert-Lewin-Platz 1
10623 Berlin
E-Mail: cirs-ains@baek.de
Tel.: 030 / 400 456 571
Fax: 030 / 400 456 455

_____ _____

Abteilungsleitung oder Institutionsleitung (Name, Vorname, Titel)

Ort, Datum

_____

Unterschrift

[Stempel / Siegel der Institution]

Für den BDA (Berufsverband Deutscher Anästhesisten) und die DGAI (Deutsche Gesellschaft für Anästhesie und Intensivmedizin) als Betreiber von CIRS-AINS, vertreten durch den Ärztlichen Geschäftsführer BDA/DGAI: Prof. Dr. Alexander Schleppers

Nürnberg, den _____

_____

Prof. Dr. A. Schleppers

Ihre unterzeichnete Vereinbarung bekommen Sie gegengezeichnet von BDA/DGAI als Kopie für Ihre Akten zurückgesendet.

CIRS-AINS: Bearbeitung der Berichte

Bei CIRSmedical Anästhesiologie (CIRS-AINS) stehen Ihnen bei der Bearbeitung der Berichte zwei Administrationsvarianten als Wahloption zur Verfügung:

Wer macht was?	**Basispaket**	**Analysepaket**
Wer?	Arbeitsgruppe aus BDA-Rechtsabteilung und Experten der Arbeitskreise BDA/DGAI **(AG-BDA/DGAI)**	
Was?		
Anonymisierung und Freigabe von Berichten und Kommentaren	AG-BDA/DGAI	AG-BDA/DGAI
Analyse und Feedback zu den Berichten	In Eigenverantwortung des Teilnehmers	AG-BDA/DGAI
Hochladen von pdfs oder Bildern	In Eigenverantwortung des Teilnehmers	AG-BDA/DGAI

Die Bearbeitung der Berichte erfolgt federführend über eine Arbeitsgruppe aus BDA-Rechtsabteilung, erfahrenen Anästhesiologen mit langjähriger CIRS-Erfahrung unterstützt durch Experten der unterschiedlichen wissenschaftlichen Arbeitskreise von BDA und DGAI **(AG BDA/DGAI)**. Bei Buchung des Basispaketes werden die eingehenden Berichte innerhalb der Geschäftsstelle von der BDA-Rechtsabteilung anonymisiert und freigeschaltet. Optional kann zusätzlich eine professionelle Analyse, Auswertung und fachliche Kommentierung durch die BDA-Rechtsabteilung gebucht werden (Analysepaket). Dies ermöglicht eine größtmögliche Fachkompetenz in der Analyse der einzelnen Fälle durch die unterschiedlichen medizinischen Fachexperten sowie die fundierte juristische Einordnung und Bewertung der Berichte, die sich auch an den bisherigen Erfahrungen aus Stellungnahmen, Entschließungen, Leitlinien und Haftpflichtfällen orientiert. Nach Freigabe der vollständig bearbeiteten Berichte erfolgt – nach einer gewissen Karenz – die Weiterleitung in die frei zugängliche nationale Datenbank CIRSmedical.de, so dass alle Internetnutzer von ihnen profitieren können.

CIRSmedical Anästhesiologie

das fachspezifische Berichtssystem für kritische Ereignisse in der Medizin

Fragebogen für die Einrichtung eines Fehlerberichts- und Lernsystems (CIRS)

Sehr geehrte Teilnehmerin, sehr geehrter Teilnehmer!

Sie nehmen an einem gemeinsamen Projekt des Berufsverbandes Deutscher Anästhesisten (BDA), der Deutschen Gesellschaft für Anästhesiologie und Intensivmedizin (DGAI) und des Ärztlichen Zentrums für Qualität in der Medizin (BÄK) teil, um in Ihrer Institution ein Berichts- und Lernsystem (CIRS) als Untergruppe des CIRS-AINS einzurichten. Um die technische Einrichtung durchführen zu können benötigen wir von Ihnen noch ein paar Angaben.
Zu diesem Zweck möchten wir Sie bitten, die folgenden Fragen zu beantworten. Alle hier gesammelten Daten werden selbstverständlich von BDA/DGAI und BÄK vertraulich behandelt.

Bitte lassen sie uns die ausgefüllten Fragebögen per E-Mail zukommen.

Wir bedanken uns schon im Voraus für Ihre Mühe!

Organisatorisches	**Administration** **Technischer Support**
BDA/DGAI Geschäftsstelle CIRS-AINS	Bundesärztekammer (BÄK)
Frau T. Rhaiem Neuwieder Str. 9 90411 Nürnberg	Frau A. Sanguino H. Herbert-Lewin-Platz 1 10623 Berlin
E-Mail: info@cirs-ains.de	E-Mail: cirs-ains@baek.de
Sekretariat: Frau S. Schmitt Tel.: 0911 / 933 78 17	Tel.: 030 / 400 456 571 Fax: 030 / 400 456 455

1. Bitte tragen Sie den Namen der teilnehmenden Institution / Krankenhaus ein

---

2. Wie wird Ihre Institution am Projekt teilnehmen? (bitte kreuzen Sie auch an, wer die Bearbeitung der eingehenden Berichte übernehmen wird)

☐ Basispaket:

Anonymisierung und Freigabe der Berichte und Nutzerkommentare durch Arbeitsgruppe aus BDA-Rechtsabteilung und Experten der Arbeitskreise BDA/DGAI.
Analyse und Feedback der Berichte und Nutzerkommentare durch CIRS-Analysegruppe Ihres Krankenhauses.

☐ Analysepaket:

Anonymisierung, Freigabe, Analyse und Feedback der Berichte und Nutzerkommentare durch Arbeitsgruppe aus BDA-Rechtsabteilung und Experten der Arbeitskreise BDA/DGAI.

1. **Bitte wählen Sie aus folgenden zwei Möglichkeiten aus über welche Methode Sie sich an dem Berichtssystem anmelden möchten. Sie können auch beide Zugangsmöglichkeiten wählen:**

   Anmeldung per IP-Adresse (IP-Adressbereich): Anhand der angegebenen IP-Adresse kann das Berichtssystem die Zugehörigkeit zu Ihrem Krankenhaus oder Ihrer Abteilung überprüfen. Es ist keine weitere Anmeldung notwendig. Von Computern die nicht dem angegebenen Adressbereich zugehören, haben Sie bei dieser Methode keinen Zugriff auf das Berichtssystem.

   Ja ☐ Nein ☐

   Bitte geben Sie die IP-Adresse (IP-Adressbereich) an:

   _____

   Anmeldung per Benutzername und Passwort: Durch Eingabe von Benutzername und Passwort ist die Anmeldung aus dem gesamten Internet an dem Berichtssystem möglich, unabhängig davon ob sich der Computer in Ihrer Abteilung befindet (z.B. von Ihrem PC zu Hause aus).

   Ja ☐ Nein ☐

   Optional können Sie ein Wunsch-Abteilungs-Login angeben (je max. 15 Zeichen):

   Benutzername:_____ Passwort: _____

   Bitte geben Sie die Adresse an, an die das Passwort per Post zugestellt werden soll:

   Name: _____

   Adresse: _____

4. Bitte tragen Sie den gewünschten Namen für das Berichtssystem ein (max. 50 Zeichen):

_____

5. Bitte geben Sie die Internetadresse an unter der Sie als Untergruppe den Zugang zum CIRS erreichen möchten (z.B. www.CIRS-AINS.de/<WunschnameXY>)

---

6. Wer ist der Ansprechpartner in Ihrer Institution/Krankenhaus für die technische Einrichtung des CIRS?

Name des Ansprechpartners: _____

E-Mail-Adresse: _____

Telefon: _____

7. Wer ist der Ansprechpartner in Ihrer Institution/Krankenhaus für die organisatorische Einrichtung?

Name des Ansprechpartners: _____

E-Mail-Adresse: _____

Telefon: _____

8. Wer ist/sind der/die Ansprechpartner der CIRS-Analysegruppe in Ihrer Institution/ Krankenhaus? (muss nicht ausgefüllt werden, wenn Sie das „Analysepaket“ gewählt haben)

Name der Ansprechpartner: _____

E-Mail-Adresse: _____

Telefon: _____

9. Wir stellen Ihnen für die Einrichtung des CIRS eine Startseite zur Verfügung (ein Beispiel dieser Seite befindet sich unter https://www.cirs-ains.de/kh-demo). Der Text auf dieser Startseite kann auf Wunsch nach Ihren Vorgaben neu gestaltet werden. Sollten Sie hierzu weitere Fragen haben, wenden Sie sich bitte an: Visionet GmbH, Am Weichselgarten 7, 91058 Erlangen, Tel.: 09131/691230. Bitte senden Sie die gewünschten Inhalte als Word-Datei an: webmaster@cirs-ains.de.

Information an alle Mitarbeiter

1) Zusicherung: Keine Nachteile durch Teilnahme an CIRS-AINS
2) Hinweis auf Verpflichtung zum Wahrheitsgrundsatz bei Meldungen

Unsere Institution möchte zur Optimierung der Patientensicherheit am bundesweiten Incident Reporting System CIRS-AINS teilnehmen. Fallberichte werden anonym über das Internet an das von BDA/DGAI und BÄK betriebene System gesendet. Durch eine möglichst umfassende und offene Darstellung abgelaufener Probleme oder kritischer Situationen und deren anschließende systematische Analyse bezüglich Ursachen und Bedingungen, hilft die Patientensicherheit systematisch zu erhöhen.

Der Sinn des CIRS-AINS ist die Erhöhung der Patientensicherheit. Es geht nicht darum „Schuldige“ zu finden.

Die Krankenhausleitung sichert hiermit allen Mitarbeitern zu, dass:

- keine Anstrengungen unternommen werden, herauszufinden, wer einen speziellen Fall berichtet haben könnte.
- selbst bei zufälliger Kenntnis der beteiligten Personen aus den Informationen im Fallbericht keine negativen Konsequenzen (Sanktionen/personalrechtliche/arbeitsrechtliche Folgen) für die Beteiligten folgen werden.
- immer versucht wird, systematische Ursachen für Probleme zu erkennen und zu verbessern, anstatt Einzelpersonen für individuelle Handlungen zur Verantwortung zu ziehen.
- das Verfassen eines Berichtes für CIRS-AINS als besonders motiviertes, verantwortungsvolles Verhalten gewertet wird und immer als positiv betrachtet wird.

Verpflichtung auf Wahrheitsgrundsatz: Die Leitung bittet darum, bei allen Meldungen den Wahrheitsgrundsatz einzuhalten. Das heißt, alle Meldungen müssen nach bestem Wissen der (zumindest subjektiv empfundenen) Wahrheit entsprechen. Dies ist für eine sinnvolle Funktion des Systems und aus juristischen Gründen z.B. im Zusammenhang mit genannten Medizingeräten notwendig.

_____

Ort, Datum

_____ _____

Unterschrift Institutionsleiter | Institution (Stempel/Siegel)

CIRSmedical Anästhesiologie

Meldung: CIRS-AINS Beauftragte

Institution: _____

Es wird empfohlen, aus allen beteiligten Berufsgruppen Beauftragte zu benennen. Idealerweise sind dies freiwillige/gewählte Mitarbeiter mit Motivation und eigenem Interesse an der Thematik. Es erscheint förderlich, je nach Abteilungsgröße, mehrere zu benennen.

CIRS- AINS Beauftragte(r)

Nr.	Name, Vorname	Titel	Beruf	Adresse	Telefon/Email

Bitte beachten: Jeder CIRS-AINS Beauftragte muss eine Verpflichtung auf das Datengeheimnis nach Art. 28 Abs. 3 S. 2 Lit. b DS-GVO (Dokument 6) unterzeichnen und an die Geschäftsstelle von BDA/DGAI zurücksenden.

BDA/DGAI Geschäftsstelle
CIRS-AINS
Neuwieder Str. 9
90411 Nürnberg

CIRSmedical Anästhesiologie

Verpflichtung auf das Datengeheimnis

gemäß Art. 28 Abs. 3 S. 2 Lit. b DS-GVO, auf das Fernmeldegeheimnis gemäß § 3 Abs. 3 Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) und auf Wahrung von Geschäftsgeheimnissen von Externen

CIRS-AINS Critical-Incident-Reporting-System von BDA/DGAI und BÄK

Verpflichtender

Verpflichteter
(Name, Vorname, Institution)

1. Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DS-GVO)

Der oben Genannte wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrecht

mäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.
Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

2. Verpflichtung auf das Fernmeldegeheimnis
Aufgrund von § 3 Abs. 3 TTDSG bin ich zur Wahrung des Fernmeldegeheimnisses verpflichtet, soweit ich im Rahmen meiner Tätigkeit für ***CIRS-AINS*** bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirke.

3. Verpflichtung auf Wahrung von Geschäftsgeheimnissen
Ich bestätige, dass ich die im Zusammenhang mit meiner Tätigkeit erlangten Unterlagen oder sonstige nicht allgemein zugängliche Informationen Dritten gegenüber vertraulich behandeln werde. Ich werde diese Unterlagen und Informationen ohne vorherige schriftliche Vereinbarung mit ***CIRS-AINS*** auch nicht für eigene gewerbliche Zwecke oder andere Auftraggeber benutzen.

Von diesen Verpflichtungen habe ich Kenntnis genommen. Ich bin mir bewusst, dass ich mich bei Verletzungen des Datengeheimnisses, des Fernmeldegeheimnisses oder von Geschäftsgeheimnissen strafbar machen kann. Das Merkblatt zur Verpflichtungserklärung mit den Abschriften der genannten Vorschriften habe ich erhalten.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Verpflichteter	Unterschrift Verpflichtender BDA/DGAI

Muster nach DS-GVO.

CIRSmedical Anästhesiologie

Merkblatt zur Verpflichtungserklärung

Art. 28 Abs. 3 S. 2 Lit. b DS-GVO

Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) …

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

…

Art. 77 DS-GVO – Recht auf Beschwerde bei einer Aufsichtsbehörde

(1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

=> Artikel: 5 Abs. 2 (Datenschutz-Management-System weist die Einhaltung nach, und kann Beschwerden stoppen)

(2) Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.

Art. 78 DS-GVO – Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde

(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

(2) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn die nach den Artikeln 55 und 56 zuständige Aufsichtsbehörde sich nicht mit einer Beschwerde befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Artikel 77 erhobenen Beschwerde in Kenntnis gesetzt hat. => Dossier: Beschwerde

(3) Für Verfahren gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.

(4) Kommt es zu einem Verfahren gegen den Beschluss einer Aufsichtsbehörde, dem eine Stellungnahme oder ein Beschluss des Ausschusses im Rahmen des Kohärenzverfahrens vorangegangen ist, so leitet die Aufsichtsbehörde diese Stellungnahme oder diesen Beschluss dem Gericht zu.

Art. 79 DS-GVO – Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

(1) Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

=> Dossier: Beschwerde, Verletzung des Schutzes

(2) Für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

=> Dossier: Niederlassung

Art. 80 DS-GVO – Vertretung von betroffenen Personen

(1) Die betroffene Person hat das Recht, **eine Einrichtung, Organisationen oder Vereinigung** ohne Gewinnerzielungsabsicht, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, **zu beauftragen, in ihrem Namen eine Beschwerde einzureichen**, in ihrem Namen die in den Artikeln 77, 78 und 79 genannten Rechte wahrzunehmen und das Recht auf Schadensersatz gemäß Artikel 82 in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.

=> Dossier: Schadenersatz

(2) Die Mitgliedstaaten können vorsehen, dass jede der in Absatz 1 des vorliegenden Artikels genannten Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der gemäß Artikel 77 zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die in den Artikeln 78 und 79 aufgeführten Rechte in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt worden sind.

=> Dossier: Öffnungsklausel, Verletzung des Schutzes

Art. 81 DS-GVO – Aussetzung des Verfahrens

(1) Erhält ein zuständiges Gericht in einem Mitgliedstaat Kenntnis von einem Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter, das vor einem Gericht in einem anderen Mitgliedstaat anhängig ist, so nimmt es mit diesem Gericht Kontakt auf, um sich zu vergewissern, dass ein solches Verfahren existiert.
(2) Ist ein Verfahren zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene zuständige Gericht das bei ihm anhängige Verfahren aussetzen.
(3) Sind diese Verfahren in erster Instanz anhängig, so kann sich jedes später angerufene Gericht auf Antrag einer Partei auch für unzuständig erklären, wenn das zuerst angerufene Gericht für die betreffenden Klagen zuständig ist und die Verbindung der Klagen nach seinem Recht zulässig ist.

Art. 82 DS-GVO – Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.
=> Artikel: 28 (Auftragsverarbeitung)
=> Dossier: Auftragsverarbeitung (Auftragnehmer)
(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er **nachweist**, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.
=> Artikel: 5 Abs. 2 (Die "Rechenschaftspflicht" weist die Einhaltung des Datenschutzes per DSMS nach.)
=> Dossier: Auftragsverarbeitung (Auftragnehmer), Nachweis
=> BDSG: § 7 ("Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.")

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den **gesamten Schaden**, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

=> Artikel: 26 Abs. 3 (Auch dort gemeinsame Verantwortung), 28 Abs. 10 (Auftragsverarbeiter wird bei Verstoß zum Verantwortlichen)

=> Dossier: Auftragsverarbeitung (Auftragnehmer)

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes **zurückzufordern**, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

=> Erwägungsgrund: 150 (Bußgeld in Unternehmensgruppe)

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

=> Erwägungsgrund: 150 (Bußgeld in Unternehmensgruppe)

Art. 83 DS-GVO – Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und j verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

=> Dossier: Zweckbindung

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen **Maßnahmen zur Minderung** des den betroffenen Personen entstandenen Schadens;

=> Artikel: 5 Abs. 2 (Die "Rechenschaftspflicht" weist die Einhaltung des Datenschutzes per DSMS nach.)

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
=> Dossier: technische und organisatorische Maßnahmen
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.
=> BDSG: § 43 ("Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen.")
(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.
(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
=> Erwägungsgrund: 150 (Bußgeld in Unternehmensgruppe)
a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.
(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
=> Erwägungsgrund: 150 (Bußgeld in Unternehmensgruppe)
a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.
(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.
=> Erwägungsgrund: 150 (Bußgeld in Unternehmensgruppe)
(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.
=> Dossier: Öffnungsklausel
(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.
(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Art. 84 DS-GVO – Sanktionen

(1) Die Mitgliedstaaten legen die Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung — insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen — fest und treffen alle zu deren Anwendung erforderlichen Maßnahmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.
=> Dossier: Geldbuße, Öffnungsklausel
=> BDSG-neu: § 42 Strafvorschriften, § 43 Bußgeldvorschriften

(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

§ 20 BDSG-neu – Gerichtlicher Rechtsschutz

(1) Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und einer Aufsichtsbehörde des Bundes oder eines Landes über Rechte gemäß Artikel 78 Absatz 1 und 2 der Verordnung (EU) 2016/679 sowie § 61 ist der Verwaltungsrechtsweg gegeben. Satz 1 gilt nicht für Bußgeldverfahren.
(2) Die Verwaltungsgerichtsordnung ist nach Maßgabe der Absätze 3 bis 7 anzuwenden.
(3) Für Verfahren nach Absatz 1 Satz 1 ist das Verwaltungsgericht örtlich zuständig, in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat.
(4) In Verfahren nach Absatz 1 Satz 1 ist die Aufsichtsbehörde beteiligungsfähig.
(5) Beteiligte eines Verfahrens nach Absatz 1 Satz 1 sind
1. die natürliche oder juristische Person als Klägerin oder Antragstellerin und
2. die Aufsichtsbehörde als Beklagte oder Antragsgegnerin.
§ 63 Nummer 3 und 4 der Verwaltungsgerichtsordnung bleibt unberührt.
(6) Ein Vorverfahren findet nicht statt.
(7) Die Aufsichtsbehörde darf gegenüber einer Behörde oder deren Rechtsträger nicht die sofortige Vollziehung gemäß § 80 Absatz 2 Satz 1 Nummer 4 der Verwaltungsgerichtsordnung anordnen.

§ 41 BDSG-neu – Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 68 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass das Landgericht entscheidet, wenn die festgesetzte Geldbuße den Betrag von einhunderttausend Euro übersteigt.
(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. Die §§ 56 bis 58, 87, 88, 99 und 100 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 69 Absatz 4 Satz 2 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass die Staatsanwaltschaft das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen kann.

§ 42 BDSG-neu – Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht
und hierbei gewerbsmäßig handelt.
(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,
1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht
und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.
(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG-neu – Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder
2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.
(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.
(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.
(4) Eine Meldung, die der Meldepflichtige nach Artikel 33 der Verordnung (EU) 2016/679 erteilt hat, oder eine nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 erfolgte Benachrichtigung darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder in § 52 Absatz 1 der Strafprozessordnung bezeichnete Angehörige des Meldepflichtigen oder Benachrichtigenden nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 44 BDSG-neu – Klagen gegen den Verantwortlichen oder Auftragsverarbeiter

(1) Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person können bei dem Gericht des Ortes erhoben werden, an dem sich eine Niederlassung des Verantwortlichen oder Auftragsverarbeiters befindet. Klagen nach Satz 1 können auch bei dem Gericht des Ortes erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat.
(2) Absatz 1 gilt nicht für Klagen gegen Behörden, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden sind.
(3) Hat der Verantwortliche oder Auftragsverarbeiter einen Vertreter nach Artikel 27 Absatz 1 der Verordnung (EU) 2016/679 benannt, gilt dieser auch als bevollmächtigt, Zustellungen in zivilgerichtlichen Verfahren nach Absatz 1 entgegenzunehmen. § 184 der Zivilprozessordnung bleibt unberührt.

Erwägungsgründe DS-GVO

(141) Jede betroffene Person sollte das Recht haben, bei einer einzigen Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthalts eine Beschwerde einzureichen und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht oder wenn die Aufsichtsbehörde auf eine Beschwerde hin nicht tätig wird, eine Beschwerde teilweise oder ganz abweist oder ablehnt oder nicht tätig wird, obwohl dies zum Schutz der Rechte der betroffenen Person notwendig ist.
Die auf eine Beschwerde folgende Untersuchung sollte vorbehaltlich gerichtlicher Überprüfung so weit gehen, wie dies im Einzelfall angemessen ist.
Die Aufsichtsbehörde sollte die betroffene Person innerhalb eines angemessenen Zeitraums über den Fortgang und die Ergebnisse der Beschwerde unterrichten.
Sollten weitere Untersuchungen oder die Abstimmung mit einer anderen Aufsichtsbehörde erforderlich sein, sollte die betroffene Person über den Zwischenstand informiert werden.
Jede Aufsichtsbehörde sollte Maßnahmen zur Erleichterung der Einreichung von Beschwerden treffen, wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.
=> Dossier: Beschwerde

(142) Betroffene Personen, die sich in ihren Rechten gemäß dieser Verordnung verletzt sehen, sollten das Recht haben, nach dem Recht eines Mitgliedstaats gegründete Einrichtungen, Organisationen oder Verbände ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes personenbezogener Daten tätig sind, zu beauftragen, in ihrem Namen Beschwerde bei einer Aufsichtsbehörde oder einen gerichtlichen Rechtsbehelf einzulegen oder das Recht auf Schadensersatz in Anspruch zu nehmen, sofern dieses im Recht der Mitgliedstaaten vorgesehen ist.

Die Mitgliedstaaten können vorsehen, dass diese Einrichtungen, Organisationen oder Verbände das Recht haben, unabhängig vom Auftrag einer betroffenen Person in dem betreffenden Mitgliedstaat eine eigene Beschwerde einzulegen, und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf haben sollten, wenn sie Grund zu der Annahme haben, dass die Rechte der betroffenen Person infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung verletzt worden sind.
Diesen Einrichtungen, Organisationen oder Verbänden kann unabhängig vom Auftrag einer betroffenen Person nicht gestattet werden, im Namen einer betroffenen Person Schadenersatz zu verlangen.
=> Dossier: Beschwerde, Schadenersatz, Verletzung des Schutzes

(143) Jede natürliche oder juristische Person hat das Recht, unter den in Artikel 263 AEUV genannten Voraussetzungen beim Gerichtshof eine Klage auf Nichtigerklärung eines Beschlusses des Ausschusses zu erheben.
Als Adressaten solcher Beschlüsse müssen die betroffenen Aufsichtsbehörden, die diese Beschlüsse anfechten möchten, binnen zwei Monaten nach deren Übermittlung gemäß Artikel 263 AEUV Klage erheben.
Sofern Beschlüsse des Ausschusses einen Verantwortlichen, einen Auftragsverarbeiter oder den Beschwerdeführer unmittelbar und individuell betreffen, so können diese Personen binnen zwei Monaten nach Veröffentlichung der betreffenden Beschlüsse auf der Website des Ausschusses im Einklang mit Artikel 263 AEUV eine Klage auf Nichtigerklärung erheben.
Unbeschadet dieses Rechts nach Artikel 263 AEUV sollte jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf bei dem zuständigen einzelstaatlichen Gericht gegen einen Beschluss einer Aufsichtsbehörde haben, der gegenüber dieser Person Rechtswirkungen entfaltet.
Ein derartiger Beschluss betrifft insbesondere die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen durch die Aufsichtsbehörde oder die Ablehnung oder Abweisung von Beschwerden.
Das Recht auf einen wirksamen gerichtlichen Rechtsbehelf umfasst jedoch nicht rechtlich nicht bindende Maßnahmen der Aufsichtsbehörden wie von ihr abgegebene Stellungnahmen oder Empfehlungen.
Verfahren gegen eine Aufsichtsbehörde sollten bei den Gerichten des Mitgliedstaats angestrengt werden, in dem die Aufsichtsbehörde ihren Sitz hat, und sollten im Einklang mit dem Verfahrensrecht dieses Mitgliedstaats durchgeführt werden.
Diese Gerichte sollten eine uneingeschränkte Zuständigkeit besitzen, was die Zuständigkeit, sämtliche für den bei ihnen anhängigen Rechtsstreit maßgebliche Sach- und Rechtsfragen zu prüfen, einschließt.
Wurde eine Beschwerde von einer Aufsichtsbehörde abgelehnt oder abgewiesen, kann der Beschwerdeführer Klage bei den Gerichten desselben Mitgliedstaats erheben.

Im Zusammenhang mit gerichtlichen Rechtsbehelfen in Bezug auf die Anwendung dieser Verordnung können einzelstaatliche Gerichte, die eine Entscheidung über diese Frage für erforderlich halten, um ihr Urteil erlassen zu können, bzw. müssen einzelstaatliche Gerichte in den Fällen nach Artikel 267 AEUV den Gerichtshof um eine Vorabentscheidung zur Auslegung des Unionsrechts — das auch diese Verordnung einschließt — ersuchen.
Wird darüber hinaus der Beschluss einer Aufsichtsbehörde zur Umsetzung eines Beschlusses des Ausschusses vor einem einzelstaatlichen Gericht angefochten und wird die Gültigkeit des Beschlusses des Ausschusses in Frage gestellt, so hat dieses einzelstaatliche Gericht nicht die Befugnis, den Beschluss des Ausschusses für nichtig zu erklären, sondern es muss im Einklang mit Artikel 267 AEUV in der Auslegung des Gerichtshofs den Gerichtshof mit der Frage der Gültigkeit befassen, wenn es den Beschluss für nichtig hält.
Allerdings darf ein einzelstaatliches Gericht den Gerichtshof nicht auf Anfrage einer natürlichen oder juristischen Person mit Fragen der Gültigkeit des Beschlusses des Ausschusses befassen, wenn diese Person Gelegenheit hatte, eine Klage auf Nichtigerklärung dieses Beschlusses zu erheben — insbesondere wenn sie unmittelbar und individuell von dem Beschluss betroffen war –, diese Gelegenheit jedoch nicht innerhalb der Frist gemäß Artikel 263 AEUV genutzt hat.

(144) Hat ein mit einem Verfahren gegen die Entscheidung einer Aufsichtsbehörde befasstes Gericht Anlass zu der Vermutung, dass ein dieselbe Verarbeitung betreffendes Verfahren — etwa zu demselben Gegenstand in Bezug auf die Verarbeitung durch denselben Verantwortlichen oder Auftragsverarbeiter oder wegen desselben Anspruchs — vor einem zuständigen Gericht in einem anderen Mitgliedstaat anhängig ist, so sollte es mit diesem Gericht Kontakt aufnehmen, um sich zu vergewissern, dass ein solches verwandtes Verfahren existiert.
Sind verwandte Verfahren vor einem Gericht in einem anderen Mitgliedstaat anhängig, so kann jedes später angerufene Gericht das Verfahren aussetzen oder sich auf Anfrage einer Partei auch zugunsten des zuerst angerufenen Gerichts für unzuständig erklären, wenn dieses später angerufene Gericht für die betreffenden Verfahren zuständig ist und die Verbindung von solchen verwandten Verfahren nach seinem Recht zulässig ist.
Verfahren gelten als miteinander verwandt, wenn zwischen ihnen eine so enge Beziehung gegeben ist, dass eine gemeinsame Verhandlung und Entscheidung geboten erscheint, um zu vermeiden, dass in getrennten Verfahren einander widersprechende Entscheidungen ergehen.

(145) Bei Verfahren gegen Verantwortliche oder Auftragsverarbeiter sollte es dem Kläger überlassen bleiben, ob er die Gerichte des Mitgliedstaats anruft, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat, oder des Mitgliedstaats, in dem die betroffene Person wohnt; dies gilt nicht, wenn es sich bei dem Verantwortlichen um eine Behörde eines Mitgliedstaats handelt, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.
=> Dossier: Niederlassung

(146) Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen.
Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist.
Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.
Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten.
Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht.
Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten.
Sind Verantwortliche oder Auftragsverarbeiter an derselben Verarbeitung beteiligt, so sollte jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden haftbar gemacht werden.
Werden sie jedoch nach Maßgabe des Rechts der Mitgliedstaaten zu demselben Verfahren hinzugezogen, so können sie im Verhältnis zu der Verantwortung anteilmäßig haftbar gemacht werden, die jeder Verantwortliche oder Auftragsverarbeiter für den durch die Verarbeitung entstandenen Schaden zu tragen hat, sofern sichergestellt ist, dass die betroffene Person einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhält.
Jeder Verantwortliche oder Auftragsverarbeiter, der den vollen Schadenersatz geleistet hat, kann anschließend ein Rückgriffsverfahren gegen andere an derselben Verarbeitung beteiligte Verantwortliche oder Auftragsverarbeiter anstrengen.
=> Dossier: Nachweis, Schadenersatz

(147) Soweit in dieser Verordnung spezifische Vorschriften über die Gerichtsbarkeit — insbesondere in Bezug auf Verfahren im Hinblick auf einen gerichtlichen Rechtsbehelf einschließlich Schadenersatz gegen einen Verantwortlichen oder Auftragsverarbeiter — enthalten sind, sollten die allgemeinen Vorschriften über die Gerichtsbarkeit, wie sie etwa in der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates (13) enthalten sind, der Anwendung dieser spezifischen Vorschriften nicht entgegenstehen.
=> Dossier: Schadenersatz

(148) Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden.
Im Falle eines geringfügigeren Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden.
Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand.
Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.
=> Dossier: Geldbuße

(149) Die Mitgliedstaaten sollten die strafrechtlichen Sanktionen für Verstöße gegen diese Verordnung, auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften, festlegen können.
Diese strafrechtlichen Sanktionen können auch die Einziehung der durch die Verstöße gegen diese Verordnung erzielten Gewinne ermöglichen.
Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes "ne bis in idem", wie er vom Gerichtshof ausgelegt worden ist, führen.

(150) Um die verwaltungsrechtlichen Sanktionen bei Verstößen gegen diese Verordnung zu vereinheitlichen und ihnen mehr Wirkung zu verleihen, sollte jede Aufsichtsbehörde befugt sein, Geldbußen zu verhängen.
In dieser Verordnung sollten die Verstöße sowie die Obergrenze der entsprechenden Geldbußen und die Kriterien für ihre Festsetzung genannt werden, wobei diese Geldbußen von der zuständigen Aufsichtsbehörde in jedem Einzelfall unter Berücksichtigung aller besonderen Umstände und insbesondere der Art, Schwere und Dauer des Verstoßes und seiner Folgen sowie der Maßnahmen, die ergriffen worden sind, um die Einhaltung der aus dieser Verordnung erwachsenden Verpflichtungen zu gewährleisten und die Folgen des Verstoßes abzuwenden oder abzumildern, festzusetzen sind.
Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff "Unternehmen" im Sinne der Artikel 101 und 102 AEUV verstanden werden.

Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen.
Das Kohärenzverfahren kann auch genutzt werden, um eine kohärente Anwendung von Geldbußen zu fördern.
Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können.
Auch wenn die Aufsichtsbehörden bereits Geldbußen verhängt oder eine Verwarnung erteilt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen nach Maßgabe dieser Verordnung verhängen.
=> Artikel: 4 Nr. 19 (Definition von Unternehmensgruppe)
=> Dossier: Geldbuße

(151) Nach den Rechtsordnungen Dänemarks und Estlands sind die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig.
Die Vorschriften über die Geldbußen können so angewandt werden, dass die Geldbuße in Dänemark durch die zuständigen nationalen Gerichte als Strafe und in Estland durch die Aufsichtsbehörde im Rahmen eines Verfahrens bei Vergehen verhängt wird, sofern eine solche Anwendung der Vorschriften in diesen Mitgliedstaaten die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen hat.
Daher sollten die zuständigen nationalen Gerichte die Empfehlung der Aufsichtsbehörde, die die Geldbuße in die Wege geleitet hat, berücksichtigen.
In jeden Fall sollten die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein.
=> Dossier: Geldbuße

(152) Soweit diese Verordnung verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei schweren Verstößen gegen diese Verordnung — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende Sanktionen vorsieht.
Es sollte im Recht der Mitgliedstaaten geregelt werden, ob diese Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind.

§ 3 TTDSG – Vertraulichkeit der Kommunikation – Fernmeldegeheimnis

(1) [1]Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. [2]Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) [1]Zur Wahrung des Fernmeldegeheimnisses sind verpflichtet

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
2. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
3. Betreiber öffentlicher Telekommunikationsnetze und
4. Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.

[2]Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) [1]Den nach Absatz 2 Satz 1 Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste oder für den Betrieb ihrer Telekommunikationsnetze oder ihrer Telekommunikationsanlagen einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation zu verschaffen. [2]Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. [3]Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. [4]Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Fernmeldegeheimnisses nicht gegenüber der Person, die das Fahrzeug führt, und ihrer Stellvertretung.

§ 206 StGB – Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die
1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekannt geworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

BDA/DGAI Geschäftsstelle
CIRS-AINS
Neuwieder Str. 9
90411 Nürnberg
Email: info@cirs-ains.de

CIRSmedical Anästhesiologie

Hinweise
im Falle eines Kontakts mit Strafverfolgungsbehörden

1) Aussageverweigerungsrecht für CIRS-AINS Beauftragte und Mitarbeiter

[Auszug aus dem juristischen Gutachten der Kanzlei Ulsenheimer]

Das Zeugnisverweigerungsrecht ist ein Berufsrecht für Angehörige der zur Zeugnisverweigerung berechtigten Berufe. Mitglieder dieser Berufsgruppen müssen deshalb vor einer Vernehmung nicht extra auf ihr Zeugnisverweigerungsrecht hingewiesen werden.

§ 53 Abs. 1 Nr. 5 StPO erkennt „Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben“, **ein weit reichendes Zeugnisverweigerungsrecht hinsichtlich der Person des Informanten, der in Hinblick auf ihre Tätigkeit gemachten Mitteilung, über deren Inhalt, den Inhalt selbst erarbeiteter Materialien und den Gegenstand berufsbezogener Wahrnehmungen an**.

CIRS-AINS ist ein der Unterrichtung von Mitarbeitern im Gesundheitswesen dienender Informations- und Kommunikationsdienst von DGAI und BDA. Die redaktionell aufbereiteten Meldungen werden der (Fach-) Öffentlichkeit zum Zwecke der Diskussion und des Erkenntnisgewinns zur Verfügung gestellt. Der Dienst dient einer allgemein zugänglichen Unterrichtung und Meinungsbildung.

Der Zeuge ist mit der redaktionellen Aufbereitung der abrufbaren Informationen befasst. Er ist wiederkehrend für den Dienst tätig.
Das Zeugnisverweigerungsrecht bezieht sich auf sämtliche Arbeitsschritte einer Publikation von der Recherche über die inhaltliche, sprachliche und technische Gestaltung bis hin zur Veröffentlichung der Mitteilung. Folge ist ein Zeugnisverweigerungsrecht hinsichtlich der Person des Einsenders der Meldung sowie deren Inhalt.

2) Es besteht ein Beschlagnahmeverbot gemäß § 97 Abs. 5 StPO

Hinsichtlich Schriftstücken, Ton-, Bild- und Datenträgern, die sich im Gewahrsam der Mitarbeiter oder der Redaktion befinden. Mindestens ist eine Versiegelung bis zur endgültigen Prüfung zu veranlassen.

Im Zweifel bitten wir um Rücksprache mit der BDA-Rechtsabteilung, Nürnberg

Kontaktdaten Sekretariat:

Gabriele Schneider-Trautmann (A-K)	Tel.: 0911 / 933 78-27	E-Mail: gschneider@bda-ev.de
Simone Schmitt (L-R)	Tel.: 0911 / 933 78-17	E-Mail: sschmitt@bda-ev.de
Filiz Özgün (S-Z)	Tel.: 0911/ 933 78-19	E-Mail: foezguen@bda-ev.de

CIRSmedical Anästhesiologie

CIRS-AINS Onlineschulung für CIRS-AINS Beauftragte

Bei Buchung des Basispaketes wird die Schulung von mindestens einem CIRS-AINS Beauftragten für die Einrichtung von CIRS-AINS in Ihrer Institution empfohlen. Wenn möglich sollten mindestens ein ärztlicher und eine pflegerischer Mitarbeiter an der Schulung teilnehmen. Ideal ist es, jeweils geschulte Mitarbeiter auf Intensivstation und im OP zu haben, damit überall Ansprechpartner verfügbar sind. Je nach Abteilungsgröße sind mehrere Mitarbeiter vorteilhaft. Generell gilt: Je mehr Mitarbeiter geschult und motiviert sind, umso effektiver wird der Start von CIRS-AINS sein. Deshalb empfehlen wir auch bei der Buchung des Analysepaketes die Teilnahme an einer CIRS-AINS Schulung.

Inhaltliche Grundlagen der CIRS-AINS Onlineschulung

- Vorstellung der BDA/DGAI Leistungen und der möglichen Zusatzoptionen
- Fehlerentstehung und -prävention: Systemansatz, fehlerprovozierende Handlungssituationen, grundlegende fehlerträchtige menschliche Eigenschaften (Human Factors)
- Einführung in das CIRS-AINS System
- Technische Aspekte der Dateneingabe und -speicherung: Datensicherheit, Zugriffsmöglichkeiten, Rechteverwaltung etc.
- Sensibilität der Aufgabe: Do's and Dont's beim Sammeln und Analysieren von Fällen.
- Konsequenzen aus CIRS-AINS: Sich aus Meldungen ergebende Aufgaben, Möglichkeiten der Umsetzung, Tipps für Unterstützung und Hilfe, rechtliche Konsequenzen für die nutzende Institution etc.
- Anonymisierung von eingehenden Fallberichten
- Rechtliche Aspekte: Zwischenfall und Unfall-Meldepflichten etc. Wahrheitsgrundsatz und Wahrheitspflicht bei den Meldungen (formale „Verpflichtung zur Wahrheitsgemäßen Mel dung"), Zeugnisverweigerungsrecht und Datensicherheit bei CIRS-AINS etc.

CIRS-AINS Basisschulung online:

www.patientensicherheit-ains.de/veranstaltungen/schulungen.html

CIRSmedical Anästhesiologie

Gebührenübersicht

(gültig ab 01.01.2010)

In nachfolgender Tabelle sind die Gebühren je Variante in Euro pro Monat (zzgl. der gesetzlichen MWSt.) in Abhängigkeit der Anzahl an ärztlichen Mitarbeiter/Innen (VK's) ersichtlich. Diese Gebühren decken die Kosten für alle Mitarbeiter der jeweiligen Abteilung ab (Ärzte, Pflegekräfte, MTAs usw., die immer mitmelden sollten). Die Anzahl der ärztlichen Mitarbeiter ist also nur die Maßzahl für die Abteilungsgröße und damit letztlich der erwarteten durchschnittlichen Anzahl eingehender Meldungen.

Der Betrag wird Ihnen einmal pro Halbjahr über den BDA in Rechnung gestellt. Die ausgewiesenen Kosten für das Analyse- und Feedback-Modul beinhalten bereits die Kosten für das Basispaket mit externer Anonymisierung). Bitte beachten Sie, dass die Gebühren aufwandsgemäß alle 12 Monate neu angepasst werden können.

Kosten / Monat zzgl. MWSt. **Anzahl ärztliche Mitarbeiter/ Innen**	**CIRS-AINS Basispaket (mit externer Anonymisierung)**	**CIRS-AINS Analysepaket (externe Analyse & Feedback inkl. externer Anonymisierung)**
bis 10	12 €	45 €
bis 30	30 €	90 €
bis 50	70 €	210 €
bis 80	120 €	360 €
> 80	170 €	510 €

CIRSmedical Anästhesiologie

Änderungsmeldung CIRS-AINS Beauftragte

Institution: _____

In meiner Institution wird sich die Zusammensetzung der CIRS-AINS Beauftragten ändern.

Ausscheidende(r) CIRS-AINS Beauftragte(r)

Nr.	Name, Vorname	Telefon / Email

Neue(r) CIRS-AINS Beauftragte(r) ab _____:

Nr.	Name, Vorname	Titel, Beruf	Adresse	Telefon/Email

Der/Die neue(n) CIRS-AINS Beauftragte(n) sind durch den/die bisherigen CIRS-AINS Beauftragten in ihre Aufgabe eingearbeitet worden. Alle Informationen über CIRS-AINS sind damit dem/n neuen CIRS-AINS Beauftragten bekannt.
Bitte beachten: Jede(r) neue CIRS-AINS Beauftragte muss eine Verpflichtung auf das Datengeheimnis (Dokument 6) unterzeichnen und an die Geschäftsstelle des BDA/DGAI zurücksenden.

BDA/DGAI Geschäftsstelle, CIRS-AINS, Neuwieder Str. 9, 90411 Nürnberg

CIRSmedical Anästhesiologie

Konformitätserklärung/Teilnahmebestätigung

Das Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten trat am 26. Februar 2013 in Kraft. Es hat zum Ziel, erstmals die Rechte von Patientinnen und Patienten in einem Gesetz zu bündeln und in wesentlichen Punkten weiterzuentwickeln. Es handelt sich um ein sog. Artikelgesetz, das Änderungen in anderen Gesetzen, hier insbesondere im Sozialgesetzbuch V (SGB V), kodifiziert.
Das PatRG misst u.a. der Etablierung einer Fehlervermeidungskultur in der medizinischen Versorgung eine große Bedeutung bei. Behandlungsfehlern soll möglichst frühzeitig vorgebeugt werden. Hierzu wurde der Gemeinsame Bundesausschuss beauftragt, Anforderungen an klinische Risikomanagement- und Fehlermeldesysteme, wie unser CIRS-AINS, zu formulieren (Art. 2 Nr. 8 PatRG) und den Schutz der meldenden Personen in solchen Systemen zu regeln (Art. 2 Nr. 7 PatRG).

Der GBA hat zunächst Mindeststandards an einrichtungsübergreifende Fehlermeldesysteme (sog. üFMS) von Krankenhäusern festgelegt (§ 136a Abs. 3 Satz 1 SGB V). Für üFMS, die in besonderem Maße geeignet erscheinen, Risiken und Fehlerquellen…zu erkennen, auszuwerten und zur Vermeidung unerwünschter Ereignisse beizutragen“ hat der GBA darüber hinaus Anforderungen bestimmt, deren Erfüllung als Grundlage für die Vereinbarung von Vergütungszuschlägen nach § 17b Abs. 1a Nr. 4 des Krankenhausfinanzierungsgesetzes (KHG) dienen (§ 136a Abs. 3 Satz 3 SGB V).

Ein Krankenhaus kann also Vergütungszuschläge nach § 17b KHG nur dann beanspruchen, wenn es nachweislich an einem Fehlermeldesystem teilnimmt, das diese über die Mindeststandards hinausgehenden Kriterien des GBA erfüllt. Die Höhe der Zuschläge wird zwischen der Deutschen Krankenhausgesellschaft, dem Spitzenverband der gesetzlichen Krankenkassen und dem Verband der privaten Krankenversicherung bundeseinheitlich vereinbart (aktuell 0,20 Cent pro vollstationären Fall).

Diese Anforderungen des GBA an üFMS sind am 5. Juli 2016 in Kraft getreten. Ein konkretes Fehlermeldesystem wird nicht vorgegeben. CIRS-AINS erfüllt diese Anforderungen in jeder Beziehung und ist daher nach §137 Abs. 1d „in besonderem Maße geeignet…, Risiken und Fehlerquellen…zu erkennen, auszuwerten und zur Vermeidung unerwünschter Ereignisse beizutragen“.

Eine Übersicht der Anforderungen des GBA und deren Umsetzung bei CIRS-AINS finden Sie hier: https://www.cirs-ains.de/files/GBA%20Anforderugnen%20%C3%BCFMS.pdf

Die Konformitätserklärung und Teilnahmebestätigung zum üFMS CIRS-AINS finden Sie hier: https://www.cirs-ains.de/files/Teilnahme%20ueFMS%20CIRS-AINS.pdf