SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

AG Cybersicherheit: 2. Sitzung
Protokollierte Sitzungspräsentation

Online-Veranstaltung (GoToMeeting)

Felix Dotzauer

Donnerstag, 10. Juni 2021 // 10:00-12:00 Uhr

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Herzlich willkommen zur 2. Sitzung der AG Cybersicherheit!

24 angemeldete Teilnehmer

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Sitzungsteilnehmer/-innen

Anrede	Titel	Vorname	Nachname	Firma oder Institution
Herr	Dr.	Daniel	Bächi	INTEGRA Biosciences AG
Herr		Irvin	Bislimi	Aesculap AG
Herr		Jesus Miguel	Cabeza	Carl Zeiss Vision GmbH
Herr		Tilo	Borchardt	GETEMED Medizin- und Informationstechnik AG
Herr		Erwin	Erkinger	SIE Solutions
Herr		Lars	Fiedler	Carl Zeiss Meditec AG
Herr		Thomas	Franke	infoteam SW AG
Herr		Tobias	Gerlach	VitalAire GmbH
Frau		Sarah	Haake-Schäfer	Carl Zeiss Vision GmbH
Herr		Andy	Pillco Lozano	MedicalCommunications GmbH
Herr		Konstantin	Koschel	Andreas Hettich GmbH & Co. KG

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Sitzungsteilnehmer/-innen

Anrede	Titel	Vorname	Nachname	Firma oder Institution
Herr		Hubertus	Lasthaus	VitalAire GmbH
Herr		Ole	Möhlmann	Domino Laser GmbH
Herr		Andreas	Rieschick	seca gmbh & co. kg.
Herr		Christian	Schmidt-Janssen	KARL STORZ SE & Co. KG
Herr	Dr.	Tobias	Schwarz	Heidelberg Engineering GmbH
Frau		Madeleine	Wendt	Domino Laser GmbH
Herr		Martin	Westphal	MedicalCommunications GmbH
Herr		Tomasz	Zdych	KARL STORZ SE & Co. KG
Herr		Felix	Dotzauer	SPECTARIS e.V.
Frau		Corinna	Mutter	SPECTARIS e.V.

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Allgemeine Regeln für das Webmeeting

Bitte beachten Sie:

1. Schalten Sie Ihr **Mikrofon bitte grundsätzlich stumm, es sei denn Sie haben eine Wortmeldung**. Bitte insbesondere bei telefonischer Zuschaltung auf die Stummschaltung achten.
2. Stellen Sie **Fragen während des Meetings bitte über den Chat**. Wir versuchen möglichst viele Fragen innerhalb der Sitzung zu behandeln/zu beantworten. Alle nicht beantworteten Fragen aus dem Chat werden in eine Q&A-Liste aufgenommen.
3. Ihre **Hinweise zu technischen Problemen** übermitteln Sie bitte auch über den Chat. Wir versuchen, Ihnen zu helfen. Sollte es Probleme geben, die sich nicht beheben lassen, wählen Sie sich bitte erneut ein oder versuchen Sie es über das Telefon oder die App. Sie sehen die Nummer bzw. den Zugangscode in Ihrer Einladung und jetzt auch im Chat.

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Kartellrechtliche Hinweise (1/3)

VERBOTE

1. **Niemals** Absprachen, Vereinbarungen treffen, Beschlüsse fassen oder auch nur Gespräche führen (besonders mit einem Konkurrenten) über alles, was wirtschaftlich sensible Themen betrifft, wie z. B. Preise, Zahlungskonditionen und Rechnungsstellungspraktiken, Produktion, Bestände, Umsätze, Kosten, zukünftige Geschäftspläne, Angebote oder Angelegenheiten in Zusammenhang mit einzelnen Lieferanten oder Kunden, Ausschluss oder kollektiven Boykott von Konkurrenten oder Zulieferern.
2. **Niemals** schriftliche Informationen, die nicht öffentlich zugänglich sind, entgegennehmen oder einen mündlichen Austausch von solchen Informationen mit Mitgliedern vereinbaren, die unter Punkt 1 fallen.
3. **Niemals** an Sitzungen ohne schriftliche Tagesordnung bzw. klare Darstellung des Zwecks teilnehmen.
4. **Niemals** an einem Informationsaustausch, über eine Marktstudie oder einem Benchmarking-Projekt teilnehmen, wenn dabei auf Informationen über einzelne Konkurrenten zugegriffen werden kann.
5. **Niemals** ohne Rechtsberatung gemeinsame Verhandlungen, Absatz- oder Einkaufsprojekte durchführen.

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

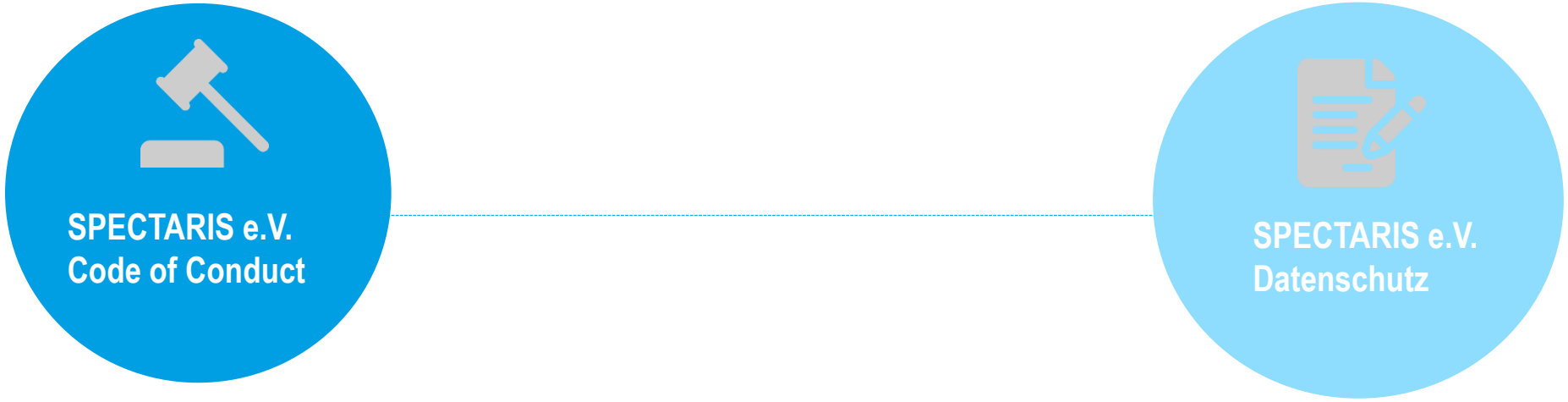
Kartellrechtliche Hinweise (2/3)

GEBOTE

1. **Bitte** lesen Sie den SPECTARIS-Verhaltenskodex!
2. **Bitte** beteiligen Sie sich an Gesprächen über Politik, Bildung, wissenschaftliche Entwicklungen, aufsichtsrechtliche Themen von allgemeinem Interessen, allgemeine Branchentrends, nicht auf Einzelunternehmen bezogene (statistische) Marktstudien oder Benchmarking-Projekte, öffentlich verfügbare Informationen oder vergangenheitsbezogene Informationen. Brechen Sie aber solche Gespräche ab und geben Sie Ihre ablehnende Haltung zu Protokoll, wenn jemand Themen anspricht, die auf der Verbotsliste genannt sind.
3. **Bitte** informieren Sie SPECTARIS, wenn Sie mit Entscheidungen nicht einverstanden sind, und bewahren Sie bei solchen Mitteilungen einen Durchschlag für Ihre Akten auf.
4. **Bitte** geben oder schicken Sie wirtschaftlich sensible Informationen, die Sie erhalten haben, zurück. Bewahren Sie keine Kopien davon auf, und erklären Sie schriftlich, dass Sie keine solchen Informationen erhalten möchten.
5. **Bitte** nehmen Sie nur dann an spontanen Treffen teil, wenn Sie wissen, dass sie gemäß Treu und Glauben einem redlichen Zweck oder allein dem geselligen Beisammensein dienen.
6. **Bitte** informieren Sie Ihre Rechtsabteilung und SPECTARIS über sämtliche Versuche der Kontaktaufnahme, die mit dem Ziel erfolgen, nicht öffentlich zugängliche Informationen auszutauschen oder das Verhalten am Markt abzustimmen.
7. **Bitten** Sie SPECTARIS darum, dass ein Rechtsbeistand an jenen Sitzungen teilnimmt, die Ihnen oder Ihrem Unternehmen zweifelhaft erscheinen.

Kartellrechtliche Hinweise (3/3)

Bitte vernehmen Sie die kartellrechtliche Hinweise auch aus den folgenden Dokumenten:



SPECTARIS-Code of Conduct zur Einhaltung kartellrechtlicher Regelungen & Datenschutzinformationen

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Agenda

- TOP 1: Begrüßung/Organisatorisches
- TOP 2: Bericht aus der Task Force US-Cloud-Anbieter
- TOP 3: Bericht aus dem Expertenkreis CyberMed
- TOP 4: Regulatorisches Update: Was ist neu seit der letzten AG-Sitzung?
  - Konsultationen & KI: Entwicklungen auf der EU-Ebene
  - Neuerungen auf nationaler Ebene
  - Übersicht: Normen & Standards der Cybersicherheit
  - Neue Veröffentlichungen
- TOP 5: Weitere Themen / Austausch

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Organisatorisches

- Rolle des AG-Sprechers: Bewerbungen willkommen!

- Zukünftige Ausrichtung der AG Cybersicherheit (post-Corona):
  - Online?
  - Präsenzveranstaltung?
  - Wechselnd zwischen Terminen online und vor Ort?
  - Hybrid?

  → **3x Sitzung online + 1x Präsenz pro Jahr**

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

TOP 2: Bericht aus der Task Force US-Cloud-Anbieter

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Task Force US-Cloud-Anbieter

- **Entstanden aus der AG Cybersicherheit, 13 Mitglieder**
- 1. Sitzung fand am 23. März statt, 2. Sitzung am 30. April, 3. Sitzung am 4. Juni
- Problemlage: Rechtsunsicherheit für Unternehmen bei der Nutzung von US-Cloud-Anbietern durch Schrems II

Ziele:

- Schaffung von **Rechtssicherheit → eindeutiger Rechtsrahmen (national & europäisch)**
- Handlungsspielraum & Wettbewerbsfähigkeit erhalten; Stand der Technik im Blick behalten (v.a. vergleichend zwischen EU & USA); Gewährleistung von Prozesssicherheit

Handlungsschritte:

- Positionspapier [in Arbeit]
- Kontaktaufnahme mit politischen Entscheidungsträgern
- Kooperation mit weiteren Verbänden, v.a. aus dem digitalen Bereich

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Aktuelle Entwicklungen: Schrems II

- **Handelsblatt-Artikel** vom 3. Mai: Brief von Verbänden und Unternehmen (u.a. SAP, Telekom, Thyssen-Krupp) an Bundeskanzleramt, Bundesjustizministerin und Bundeswirtschaftsminister: Einforderung von Rechtssicherheit bei der Nutzung von US-Cloud-Services
- Reaktion von staatlicher Seite: **Round-Table-Gespräch** zwischen BMI, BMWi, Datenschutzbehörden und Vertretern aus der Wirtschaft am 11. Juni
- 6. Mai: Microsoft stellt „EU Data Boundary“ vor: Ermöglichung von Datenspeicherung und –verarbeitung in der Microsoft-Cloud - ausschließlich in der EU → Datenschützer sind jedoch skeptisch
- 27. Mai: European Data Protection Supervisor (EDPS) startet EU-interne Untersuchung: *„one regarding the use of cloud services provided by Amazon Web Services and Microsoft under Cloud II contracts by European Union institutions, bodies and agencies (EUIs) and one regarding the use of Microsoft Office 365 by the European Commission”*

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Aktuelle Entwicklungen: Schrems II

1. Juni: Aufsichtsbehörden überprüfen verstärkt DSGVO-Einhaltung bei Unternehmen (heise.de):

„Konkret kontaktieren die Aufsichtsbehörden von Berlin, Hamburg, Brandenburg, Bremen, Niedersachsen, Rheinland-Pfalz, Baden-Württemberg, Bayern und des Saarlandes ausgewählte Unternehmen und befragen sie zu festgelegten Themen. Der gemeinsame Fragenkatalog, der als Basis dient, umfasst etwa die Themen E-Mail-Versand, Hosting von Internetseiten, Webtracking, Verwaltung von Bewerberdaten und konzerninterner Austausch von Kunden- und Beschäftigtendaten. Die einzelnen Behörden entscheiden selbst, welche Themenbereiche sie überprüfen und ob die Fragen eventuell an regionale Besonderheiten anzupassen sind.“

→ **Screening** folgt: Ein gemeinsamer Fragenkatalog der Datenschutzbehörden oder je nach Bundesland unterschiedlich?

4. Juni: Überarbeitete Standardvertragsklauseln der EU-Kommission, die bei der Datenübermittlung in die USA angewendet werden können

→ **Dennoch: Einzelfallprüfung & großer Aufwand für Unternehmen**

→ **Politische Lösungen (Angemessenheitsbeschlüsse) wären für dauerhafte Rechtssicherheit notwendig**

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Aktuelle Entwicklungen: Schrems II

- Beteiligung an einem Round Table-Gespräch zwischen Verbänden, Datenschutzbehörden und dem BMWi / BMI am **11. Juni**

Eingereichte Fragen:

- Inwieweit wird in Verbindung mit Schrems II eine Harmonisierung der DSGVO-Auslegung und –Anforderungen innerhalb Deutschlands angestrebt, um eine möglichst rechtssichere Situation für Unternehmen zu schaffen, die in mehreren Bundesländern agieren?
- Inwieweit wird in Verbindung mit Schrems II eine Harmonisierung der DSGVO-Auslegung und –Anforderungen innerhalb der Europäischen Union angestrebt, um nationale „Insellösungen“ zu vermeiden?
- Mehrere Landesdatenschutzbehörden haben jüngst offizielle Kontrollmaßnahmen angekündigt. Ausgewählte Unternehmen sollen einen Fragenkatalog zugesandt bekommen. Handelt es sich hierbei um einen gemeinsamen Fragenkatalog oder wird dieser je nach Bundesland unterschiedlich gestaltet sein?
- Schafft die Nutzung der kürzlich von der EU-Kommission aktualisierten Standardvertragsklauseln ausreichende Rechtssicherheit bei der Nutzung von Cloud-Anbietern aus den USA?
- Ist ein neuer Angemessenheitsbeschluss zwischen EU und USA absehbar? Und falls ja, wann?

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Positionspapier (& weiteres Vorgehen)

- Priorität nach dem Round-Table (& MDR-Geltungsbeginn)

Vorschlag eines „Schreibplans“:

- Fortsetzung der Textarbeit (Einarbeitung von Kommentaren + Einfügung von weiteren Infos aus dem Round-Table Gespräch): ab 14.6.
- Zusendung eines überarbeiten Entwurfs zur Finalisierung: Ende Juni/Anfang Juli
- Gleichzeitig: Kontaktaufnahme mit weiteren Verbänden vom Round-Table-Gespräch, ggf. Kooperationsmöglichkeit → gemeinsames Schreiben

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

TOP 3: Bericht aus dem Expertenkreis CyberMed

Der Expertenkreis CyberMed (EK CyberMed) in der Allianz für Cyber-Sicherheit (ACS) ist ein vom BSI betreuter Zusammenschluss von Vertretern von Industrie, Anwendern und Behörden, die sich aktiv mit dem Thema Cybersicherheit von Medizintechnik befassen.

Letzte Sitzung: 17. Mai 2021

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Expertenkreis CyberMed: Gesprächspunkte der letzten Sitzung (17. Mai)

- Vorstellung Beschleunigte Sicherheitszertifizierung (Dr. Helge Kreutzmann, BSI)
- Entwurf „Leitfaden zum Umgang mit Informationen über Schwachstellen der Informationssicherheit vernetzbarer Medizingeräte“ → mögliche Publikation des Leitfadens (erarbeitet vom ZVEI) im Rahmen der Allianz für Cybersicherheit
- BSI-Projekt ManiMed/BSI-Aktivitäten:
  - Verabschiedung von Frau Dr. Truxius / neuer Ansprechpartner: Herr Dr. Krupp
  - Neues Projekt: **„eMergent – Sicherheit von Medizinprodukten im Rettungswesen“**
- Weiteres Vorgehen: ggf. zukünftige Öffnung des EK CyberMed für einzelne Vertreter von Benannten Stellen (in Diskussion)

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Beschleunigte Sicherheitszertifizierung (BSZ)

„Die "Beschleunigte Sicherheitszertifizierung" (BSZ) ermöglicht es Herstellern, die Sicherheitsaussage ihres Produktes durch ein unabhängiges Zertifikat bestätigen zu lassen. *Das Zertifizierungsschema basiert auf planbaren Evaluierungslaufzeiten und hält den Aufwand für den Produkthersteller insbesondere im Bereich der Dokumentation überschaubar. Die Evaluierung folgt einem risikogetriebenen Ansatz, welcher ein hohes Niveau an Vertrauen in die Sicherheitsaussagen schafft. Momentan richtet sich die Zertifizierung primär an Produkte aus dem Bereich der Netzwerkkomponenten.* ***Weitere Geltungsbereiche werden in naher Zukunft erschlossen.“***

- Evaluierung durch eine vom BSI anerkannte Prüfstelle
- BSZ ist kompatibel zur französischen CSPN (gegenseitige Anerkennung in Vorbereitung)
- Basis für die Integration auf europäischer Ebene in zukünftige CSA [EU Cyber Security Act]-Schemata
- Austausch zwischen BSI und Medizinprodukteherstellern soll hier intensiviert werden

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Unterscheidung: Sicherheitszertifizierung / Sicherheitskennzeichen

- Sicherheitszertifizierung:
  - BSI als nationale Cybersicherheitszertifizierungsbehörde gemäß des Cyber Security Acts (EU 2019/881)
  - Nachweis des Herstellers, dass ein Produkt definierten Sicherheitsanforderungen entspricht
  - Unabhängige Prüfung durch das BSI und zertifizierten Prüfstellen erforderlich
  - Zertifizierungswege: Common Criteria (CC), Signaturgesetz (SigG), Technische Richtlinie (TR) & BSZ
- IT-Sicherheitskennzeichen:
  - Freiwillige Selbsterklärung (im Sinne des Verbraucherschutzes) → Herstellererklärung + BSI-Sicherheitsinformation
  - auf Produkt oder Verpackung angebracht, auch elektronischer Verweis möglich
  - Nach Erteilung des IT-Sicherheitskennzeichens besitzt das BSI die Prüfbefugnis, ob die erklärten Anforderungen auch fortlaufend eingehalten werden → Marktüberwachung
  - Aktuell noch im Aufbau

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

TOP 4: Regulatorisches Update: Was ist neu seit der letzten AG-Sitzung?

- Konsultationen & KI: Entwicklungen auf der EU-Ebene
- Neuerungen auf nationaler Ebene
- Übersicht: Normen & Standards der Cybersicherheit
- Neue Veröffentlichungen

Entwurf: Richtlinie über Maßnahmen für ein Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 („NIS 2“)

Quelle: EU-Kommission: Factsheet NIS 2

- Kernpunkte des NIS 2-Richtlinienentwurfs:
  - striktere Cybersicherheitsanforderungen an essentielle Akteure in der EU
  - Stärkung der Abwehrfähigkeit öffentlicher und privater Sektoren → Erweiterung des Geltungsbereich der „essential entitities“, darunter: Hersteller von Medizinprodukten
  - Außerdem: abgeschwächte Anforderungen für „important entities“: weitere Medizinprodukte-Unternehmen & IVD-Hersteller
- Öffentliche Konsultation der EU-KOM lief bis zum 21. März
- Bis Ende Februar hatten wir die Möglichkeit Rückmeldung via MTE einzugeben → 18.03.2021: MTE Positionspapier
- 30.04.2021: Boryana Hristova, DG CONNECT: Präsentation zu NIS 2-Grundlagen in der Cyber Security WG von MTE

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Two regulatory regimes

	Essential entities	Important entities
Scope	Scope of NIS1 + certain new sectors	Most new sectors + certain entities from NIS1 scope
Security requirements	Risk-based security obligations, including accountability of top management	
Reporting obligations	Significant incidents and significant cyber-threats	
Supervision	Ex-ante + ex post	Ex-post
Sanctions	Minimum list of administrative sanctions, including fines. Only for essential entities: *ultima ratio* possibility to suspend authorisation or impose temporary ban on managerial duties	
Jurisdiction	General rule: MS where the service is provided Exception: Main establishment + ENISA registry for certain digital infrastructures and digital providers	

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Frage der Abgrenzung: Welche Medizintechnik-Unternehmen fallen unter „essential“, welche unter „important entities“? (Annex I & II, NIS 2-Entwurf)

ESSENTIAL ENTITIES

— Entities carrying out research and development activities of medicinal products referred to in Article 1 point 2 of Directive 2001/83/EC ([21])

— Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2

— Entities manufacturing medical devices considered as critical during a public health emergency (‘the public health emergency critical devices list’) referred to in Article 20 of Regulation XXXX[22]

[22] [Regulation of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal produces and medical devices, reference to be updated once the proposal COM(2020)725 final is adopted]

IMPORTANT ENTITIES

(a) Manufacture of medical devices and in vitro diagnostic medical devices	Entities manufacturing medical devices referred to in Article 2 point 1 of Regulation (EU) 2017/745([32]), and entities manufacturing in vitro diagnostic medical devices referred to in Article 2 point 2 of Regulation (EU) 2017/746 ([33]) with exception of entities manufacturing medical devices mentioned in Annex 1, point 5.

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Frage der Abgrenzung: Welche Medizintechnik-Unternehmen fallen unter „essential“, welche unter „important entities“?

Wichtige Zusatzinformation:

*„The proposal foresees a **general exclusion of micro and small entities from the NIS scope** and a lighter ex-post supervisory regime applied to a large number of the new entities under the revised scope (so-called important entities).”* (S. 8 des NIS 2-Entwurfs)

→ **Microunternehmen/kleine Unternehmen sollen also nicht unter das NIS 2-Framework fallen**

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

EU-Gesetzespaket zu Künstlicher Intelligenz (KI)

- 21. April 2021: EU-KOM stellt erstmals den Plan für eine umfassende KI-Gesetzgebung für Europa vor, darunter:

  1.) ein einheitlicher Rechtsrahmen in Form einer geplanten KI-Verordnung mit risikobasiertem Ansatz;

  2.) ein mit den EU-Mitgliedstaaten koordinierter Plan als europäisches Konzept für Exzellenz in der KI;

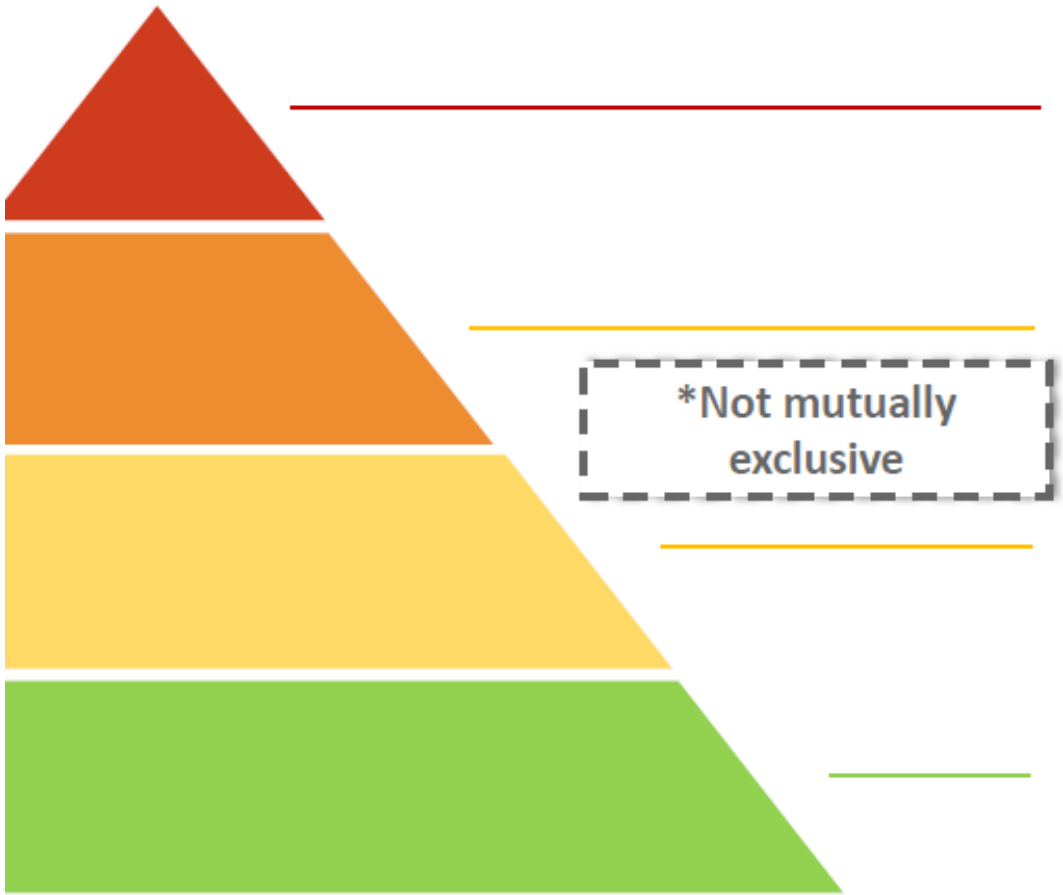
  3.) ein Vorschlag für eine Maschinenverordnung, welche die bislang geltende Maschinenrichtlinie ersetzen soll.

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Genaueres zum KI-Verordnungsentwurf

- Horizontaler Rechtsrahmen für KI-Anwendungen mit risikobasiertem Ansatz:
  - Besonders gefährliche KI-Praktiken, wie z.B. Social Scoring, sollen verboten werden.
  - Bevor KI-Systeme mit hohem Risiko auf dem Unionsmarkt in Verkehr gebracht werden dürfen, müssen eine Reihe von horizontalen verbindlichen Anforderungen für vertrauenswürdige KI erfüllt werden, wie z.B:
    - die Einrichtung eines Qualitätsmanagement- und Marktbeobachtungssystems,
    - die Durchführung eines **Konformitätsbewertungsverfahrens durch zugelassene Zertifizierungsstellen (Benannte Stellen)**,
    - die Ausstellung einer **Konformitätserklärung und CE-Kennzeichnung**,
    - **Registrierungspflichten**, und
    - die Etablierung einer **EU-Datenbank** für eigenständige **KI-Systeme mit hohem Risiko**.
- **Auch KI-Systeme von Medizinprodukten und sicherheitsrelevante Komponenten von Maschinen könnten unter die Kategorie „KI-System mit hohem Risiko“ fallen.** Auch wenn hier keine neue KI-Zertifizierungsebene geplant ist, sollen die Konformitätsbewertungen zum Thema KI über Benannte Stellen erfolgen.

A risk-based approach



*Not mutually exclusive

Unacceptable risk
e.g. social scoring
— **Prohibited**

High risk
e.g. recruitment, medical devices
— **Permitted** subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk
'Impersonation' (bots)
— **Permitted** but subject to information/transparency obligations

Minimal or no risk
— **Permitted** with no restrictions

European Commission

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Genaueres zum KI-Verordnungsentwurf

- Für KI-Systeme mit niedrigerem Risiko („other risk“) sind Transparenzpflichten vorgesehen.
- Für KI-Systeme der niedrigsten Risikostufe sollen keine verpflichtenden Vorgaben gelten. Hier ist stattdessen ein freiwilliger Code of Conduct vorgesehen.
- Des Weiteren soll ein **Beratungsgremium („European Artificial Intelligence Board“) für die Kommission** errichtet werden.
- Durch „Regulatory sandboxes“ und die Förderung von KMU und Start-Ups soll die KI-Verordnung zusätzlich innovationsfördernd wirken.

Die EU-Kommission bittet nun, als Ergänzung zur aktuellen Gesetzgebungsdebatte zwischen dem Europäischen Parlament und Ministerrat, um weitere Anmerkungen zur geplanten KI-Verordnung. Bis zum 6. August 2021 können Rückmeldungen an die Kommission über die Konsultationsseite erfolgen.

SPECTARIS-interner Konsultationsprozess lief bis Ende Mai, bislang haben wir jedoch keine Rückmeldung erhalten. Falls Sie Input für uns haben sollten, gerne via Mail an regulatoryaffairs@spectaris.de.

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Frage zur Unterscheidung: Was ist mit Medizinprodukten mit kleinen/harmlosen KI-Elementen? Fallen diese ebenfalls unter „high risk“ oder gibt es eine Abstufung?

- Bislang ist uns keine mögliche Abstufung bekannt. Vielmehr verweist der Verordnungstext eher auf eine durchgehende „high-risk“-Einstufung von Medizinprodukten mit KI-Elementen:

„(30) As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain Union harmonization legislation, it is appropriate to classify them as high-risk under this Regulation if the product in question undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are […] ***medical devices, and in vitro diagnostic medical devices.***

(31) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered ‘high-risk’ under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is notably the case for ***Regulation (EU) 2017/745*** *of the European Parliament and of the Council and* ***Regulation (EU) 2017/746*** *of the European Parliament and of the Council, where a third-party conformity assessment is provided for medium-risk and high-risk products.”*

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Cybersicherheitsanforderungen in der MDR

- **MDR-Geltungsbeginn: 26. Mai 2021**
- MDR Anhang I, 17.2.:

  „Bei Produkten, zu deren Bestandteilen Software gehört, oder bei Produkten in Form einer Software wird die Software entsprechend dem Stand der Technik entwickelt und hergestellt, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschließlich der Informationssicherheit, der Verifizierung und der Validierung zu berücksichtigen sind.“
- MDR Anhang I, 17.4.:

  „Die Hersteller legen Mindestanforderungen bezüglich Hardware, Eigenschaften von IT-Netzen und IT-Sicherheitsmaßnahmen einschließlich des Schutzes vor unbefugtem Zugriff fest, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind.“
- Außerdem: MDCG 2019-16: “Guidance on Cybersecurity for medical devices”

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Neuerungen auf nationaler Ebene: IT-Sicherheitsgesetz 2.0

- Detektion und Abwehr: Das BSI erhält verstärkte Kompetenzen bei der Detektion von Sicherheitslücken und der Abwehr von Cyber-Angriffen. So kann das BSI als zentrales Kompetenzzentrum der Informationssicherheit die sichere Digitalisierung gestalten und unter anderem Mindeststandards für die Bundesbehörden verbindlich festlegen und effektiver kontrollieren.
- Der Kreis der kritischen Infrastrukturen wird um weitere Sektoren erweitert (zum Beispiel Rüstungshersteller oder Unternehmen mit besonders großer volkswirtschaftlicher Bedeutung) – hier sind bestimmte IT-Sicherheitsmaßnahmen umzusetzen, im Informationsaustausch mit dem BSI. → Gesundheitswesen fällt bereits unter kritische Infrastruktur, primär Kliniken
- **Grundsätzliche Befugniserweiterung für das BSI**
- Einführung eines IT-Sicherheitskennzeichens absehbar

Neuerungen auf nationaler Ebene:
eHealth

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

DVG: Digitale-Versorgung-Gesetz [incl. The Fast-Track process for digital Health applications (DiGA) according to § 139e SGB V - App on prescription]

19.12.2019

DiGAV - Digitale-Gesundheitsanwendungen-Verordnung
Scope: e-Health applications that meet the essential requirements of functionality, security, quality, privacy and data protection and can demonstrate a positive impact on care

20.04.2020 (Veröffentlichung im Bundesgesetzblatt)

BSI TR-03161 - Sicherheitsanforderungen an digitale Gesundheitsanwendungen
Technische Richtlinie

15.04.2020

Das **Fast-Track-Verfahren** für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V
Ein Leitfaden für Hersteller, Leistungserbringer und Anwender des BfArM

17.04.2020

Patientendaten-Schutzgesetz – PDSG (Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur)

20.10.2020 (Inkrafttreten) / Wirksam ab Januar 2021

Digitale Versorgung und Pflege-Modernisierungsgesetz (DVPMG) (3. Digitalisierungsgesetz)

Mai 2021: Verabschiedung

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Übersicht: Normen der Cybersicherheit

- DIN EN ISO 13485:2016-08 Medizinprodukte - Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke (ISO 13485)
- DIN EN ISO 14971:2013-04 Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte (ISO 14971)
- DIN EN 60601-1:2013-12 Medizinische elektrische Geräte - Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale (IEC 60601-1)
- DIN EN 62304:2016-10 Medizingeräte-Software - Software-Lebenszyklus-Prozesse (IEC 62304)
- DIN EN 62366:2008-09 Medizinprodukte - Anwendung der Gebrauchstauglichkeit auf Medizinprodukte (IEC 62366)
- ISO/TR 80002-2:2017-06 Medizinische Gerätesoftware - Teil 2: Validierung von Software zur Verwendung in der Qualitätssicherung für medizinische Geräte (ISO TR 80002-2)
- DIN EN 82304-1:2018-04 Gesundheitssoftware - Teil 1: Allgemeine Anforderungen für die Produktsicherheit (IEC 82304)
- UL 2900-1: Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements [2017]

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Übersicht: Normen der Cybersicherheit

- NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations [ENTWURF, Sep. 2020]
- NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management (ERM) [Okt. 2020]
- NIST Cybersecurity Practice Guide SP 1800-30 Securing Telehealth Remote Patient Monitoring Ecosystem [ENTWURF, Nov. 2020]
- Standard GB/T 35273-2020 on Information Security Technology - Personal Information Security Specification (UK)
- **AAMI TIR57:2016/(R)2019 Principles for medical device security—Risk management**
- **IEC TR 60601-4-5:2021: Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications**
- **ISO 81001-1:2021: Health software and health IT systems safety, effectiveness and security — Part 1: Principles and concepts**
- **ISO/IEC TS 27110:2021: Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines**

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Standards/Guidance-Dokumente

National:

- BSI TR-03161: Sicherheitsanforderungen an digitale Gesundheitsanwendungen (15.04.2020)
- BSI: Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte (2018)
- Allgemeine BSI-Standards: 100-4; 200-1; 200-2; 200-3; 200-4
- BSI IT-Grundschutz-Kompendium 2021

EU:

- ENISA: Guidelines for Securing the Internet of Things (09.11.2020)
- MDCG 2019-16: Guidance on Cybersecurity for medical devices (April 2019)

International:

- IMDRF: Principles and Practices for Medical Device Cybersecurity (18.03.2020)

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Weitere interessante Links/Ressourcen

- Expertenkreis CyberMed: Sicherheit von Medizinprodukten: Leitfaden zur Nutzung des MDS2 aus 2019 (05.11.2019)
- Empfehlenswert: **Fragenkatalog „IT-Sicherheit bei Medizinprodukten“ des IG-NB** (Version 3, Stand: 06.11.2020)
- DIN/DKE/VDE: Cybersecurity Navigator (13.11.2020)
- DIN/DKE: Deutsche Normungsroadmap Künstliche Intelligenz (30.11.2020)
- **VDE: Neue Normen in der Medizintechnik** (Stand: April 2021; inklusiver vieler Cybersecurity-Normen)
- **CEN/CENELC: Neues Joint Technical Committee zu „Artificial Intelligence“: CEN-CLC/JTC 21**
- **20. Mai 2021: *DIN und DKE gründen Gemeinschaftsgremium „Cybersecurity“ (Pressemeldung):***

  „Damit werden die Kompetenzen im Bereich Cybersicherheits-Normung in Deutschland zukünftig gebündelt. Die deutschen Stakeholder aus Wirtschaft, Wissenschaft, öffentlicher Hand und Verbraucherschutz erhalten bei den zu erwartenden Normungs-aktivitäten durch bevorstehende EU-Regulierungen so besseren Zugang zur Mitgestaltung. […] Die nationalen Aktivitäten zur Bearbeitung europäischer Normungsvorhaben von CEN CENELEC Joint Technical Committe 13 und ETSI Technical Committee Cyber werden daher ab sofort normenausschussübergreifend über das neue DIN DKE Gemeinschaftsgremium „Cybersecurity“ gesteuert.“

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Übersicht: Leitfäden der Cybersicherheit

Das kanadische Guidance-Dokument wird empfohlen.

Land	Guidance-Dokumente
USA	Draft Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2018)
	Final Guidance: Postmarket Management of Cybersecurity in Medical Devices (2016)
	Final Guidance: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (2014)
	Final Guidance: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (2005)
China	Draft Technical guideline on medical device cybersecurity, Version II (2020)
EU	MDCG 2019-16: Guidance on Cybersecurity for medical devices (2019)
Kanada	Guidance Document: Pre-market Requirements for Medical Device Cybersecurity (2019)
Brasilien	Guidance No. 38/2020: Principles and Practices of Cybersecurity in Medical Devices (2020)
Australien	Medical device cyber security guidance for industry (2019)
Südkorea	South Korean Guidelines for Medical Device Cybersecurity Management (2018)
Japan	Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1 (2018) & Recent Trends (2020)
Saudi-Arabien	Guidance to Pre-Market Cybersecurity of Medical Devices (2019)
Taiwan	Guidance on Management of Cybersecurity in Medical Devices for Manufacturers (2019)
Singapur	Information Technology Standards - Council Technical Reference 67: Medical device cybersecurity (2018)
Weiteres	IMDRF: Principles and Practices for Medical Device Cybersecurity (2020)

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Neue Veröffentlichung: BSI IT-Grundschutz-Kompendium 2021

- Veröffentlicht im Februar 2021, ca. 800 Seiten
- Wird jährlich aktualisiert
- Fokus auf: Elementare Gefährdungen; Prozess-Bausteine; System-Bausteine
- IT-Grundschutz-Bausteine: zehn unterschiedliche Schichten, thematisch von Anwendungen (APP) über Industrielle IT (IND) bis hin zu Sicherheitsmanagement (ISMS)

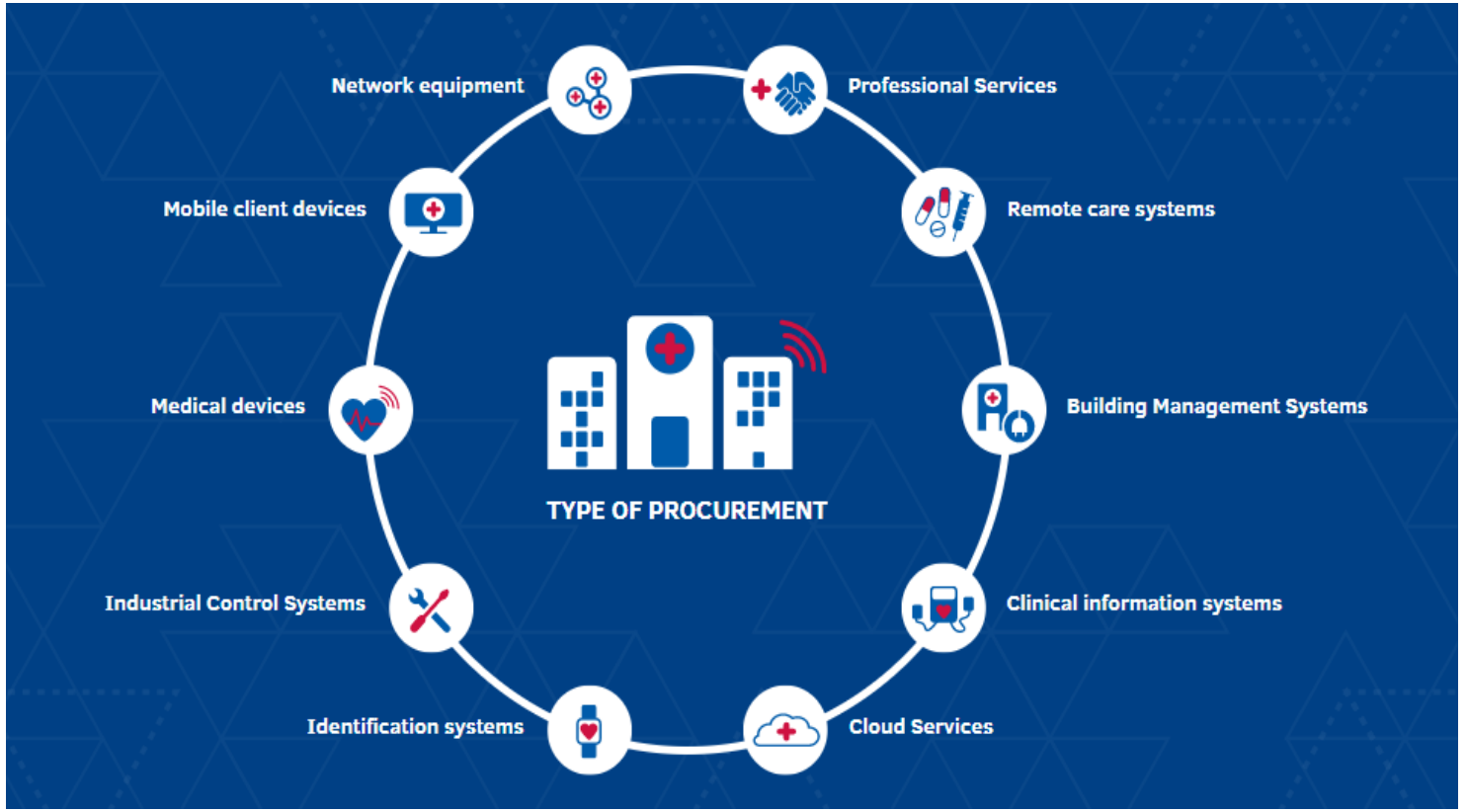
SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Neue Veröffentlichung: ENISA Online-Tool

Online-Tool der ENISA:

„Good practices for the security of healthcare services“

→ Aufbauend auf der Publikation „Procurement Guidelines for Cybersecurity in Hospitals” (Feb. 2020)



SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

ENISA: “Cloud Security for Healthcare Services”

- Hohe Vulnerabilität des Gesundheitssektors im Cyberspace: stetige Cyberangriffe → parallel zu zunehmender Digitalisierung (Telemedizin, ePA, etc.) & Covid-19-Pandemie
- Untersuchung der Sicherheit & Risiken von Cloud-basierter Technologie von besonderer Bedeutung
- Studie über Cloud-Sicherheitspraktiken & Aspekte, die bei der Beschaffung von Cloud-Diensten von Relevanz sind.
- Präsentation allgemeiner Praktiken für IT-Fachleute, um Sicherheit in der Cloud zu etablieren und aufrechtzuerhalten.
- Identifizierung relevanter Bedrohungen und Risiken für Cloud-Dienste
- Darstellung aus drei praxisorientierten Anwendungsfällen (darunter: **Medizinprodukte**)

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

TOP 5: Weitere Themen / Austausch

- Gaia-X:
  - Aktueller Stand
  - Im Einklang mit oder im Gegensatz zu laufenden gesetzlichen Initiativen?

→ **Für die nächste Sitzung ist ein Expertenvortrag zum Thema GAIA-X geplant, die Recherche zu möglichen Gastrednern läuft**

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

RA-Gremien: Termine 2021

Datum, Ort	Gremium / Event
15.06.2021, online	AG Umweltrecht
14.09.2021, online	AG IVD
15.09.2021, online	AG MDR
Okt. / Nov. 2021, online	AG Internationaler Marktzugang
Okt. / Nov. 2021, online	AG Cybersicherheit
09.11.2021, online	AG MDR
10.11.2021, online	AG IVD
24.11.2021, Berlin	RFMT-Wintersitzung
25.11.2021, Berlin	AG Vigilanz (geblockt)

SPECTARIS
Deutscher Industrieverband für Optik, Photonik, Analysen- und Medizintechnik

Vielen Dank für Ihre Aufmerksamkeit!
Bleiben Sie gesund!