Leitfaden zur Etablierung eines Cyber-Bündnisses

Anhang 1 Organisation und juristische Aspekte

ALLIANZ Industrie 4.0 BADEN-WÜRTTEMBERG

Anhang 1: Organisation und juristische Aspekte

A. Organisation

1. Organisation unter Beachtung der kartellrechtlichen Fusionskontrolle

Die Anwendbarkeit von Fusionskontrollrecht (also die reine Frage, ob eine Anmeldung erforderlich ist) richtet sich sowohl nach den Aufgreifschwellen des jeweiligen nationalen Rechts als auch nach der Organisationsform und Struktur des Zusammenschlusses im konkreten Einzelfall. In Bezug auf die angedachten Cyber-Bündnisse (im Sinne einer Wabenstruktur) könnte eine fusionskontrollrechtliche Anmeldung für die Entstehung sowie (ggf. zusätzlich) nachgelagerte strukturelle Veränderung eines einzelnen Cyber-Bündnisses bzw. einer Wabe je nach Einzelfall notwendig sein. Auch ein Zusammenschluss zwischen mehreren Cyber-Bündnissen bzw. Waben hin zu einem größeren Cyber-Bündnis könnte je nach konkreter Ausgestaltung eine Fusionskontrolle erfordern.

Die gesetzlichen Aufgreifschwellen sind gewöhnlich Umsatzschwellen, können aber auch (insbesondere alternativ) Marktanteile im betroffenen Markt oder das Erlangen einer bestimmten Marktstellung, ferner der Wert von Vermögenswerten in der betreffenden Jurisdiktion etc. sein. Die Kriterien beziehen sich grundsätzlich auf die gesamte jeweilige Unternehmensgruppe (alle von der obersten Muttergesellschaft oder Person der Gruppe kontrollierten Unternehmen). Im gröberen Sinne gilt zusammenfassend: Je wettbewerblich stärker, aktiver und/oder präsenter ein oder mehrere am Zusammenschluss involvierte Unternehmen in einem Land sind, desto höher ist die fusionskontrollrechtliche Relevanz.

In Bezug auf ein Cyber-Bündnis ist Deutschland als schwerpunktmäßige Jurisdiktion wie folgt im Überblick zu skizzieren:

Eine Anmeldepflicht besteht, wenn ein Zusammenschluss im Sinne des Gesetzes erfolgt und die Unternehmen bestimmte Umsatzschwellen überschreiten.

Als Zusammenschluss anmeldepflichtig können solche durch Anteilserwerb (stets bei formaler Überschreitung der Grenze von 25 % oder 50 % der Anteile), Erwerb wesentlichen Vermögens, Kontrollerwerb (allgemein die faktische oder rechtliche Möglichkeit, Einfluss auf die strategischen Entscheidungen eines Unternehmens ausüben zu können – auch mittelbar oder gemeinsam mit einem anderen Unternehmen) oder Erlangung der möglichen Ausübung wettbewerblich erheblichen Einflusses auf ein anderes Unternehmen sein. Daran gemessen kommt in Bezug auf ein Cyber-Bündnis, je nach rechtlicher Ausgestaltung, vorrangig die Gründung oder Entwicklung hin zu einem Gemeinschaftsunternehmen in Betracht (d. h. mindestens zwei Unternehmen erwerben gleichzeitig oder nacheinander 25 % oder mehr der Anteile an einem Unternehmen). Gründen beispielsweise also bis zu vier Unternehmen mit paritätischer Beteiligung eine GmbH als Vehikel für ihre Wabe, ist die Gründung der GmbH beim Bundeskartellamt anmeldepflichtig, wenn die Umsatzaufgreifschwellen erreicht werden.

Die wesentliche Umsatzschwelle nach deutschem Recht erfasst Zusammenschlüsse, in welchen im letzten abgeschlossenen Geschäftsjahr (1.) alle beteiligten Unternehmen gemeinsam weltweit mehr als EUR 500 Mio. und (2.) mindestens ein beteiligtes Unternehmen in Deutschland mehr als EUR 50 Mio. und (3.) mindestens ein weiteres in Deutschland mehr als EUR 17,5 Mio. an Nettoumsatzerlösen erzielt haben (eine Fusionskontrolle käme auch in Betracht, wenn alternativ zu 3. der Transaktionswert EUR 400 Mio. übersteigt). Der Industriezweig/Geschäftsbereich, in dem der Umsatz erzielt wurde, spielt keine Rolle. Die geografische Zuordnung richtet sich gewöhnlich nach dem Sitz des Kunden.

Im Falle einer Anmeldepflicht beim Bundeskartellamt (sowie auch weit überwiegend in anderer Jurisdiktion) ist eine Freigabe durch das Bundeskartellamt zwingend abzuwarten. Ein betroffenes Cyber-Bündnis dürfte in dieser Zeit nicht (auch nur teilweise) umgesetzt werden. In Bezug auf Deutschland erhöht sich im Allgemeinen das Risiko einer Fusionskontrolle mit zunehmender Ausgestaltung des (rechtsverbindlichen) Organisationsmaßes, insbesondere im Falle der Gesellschaftsgründung wie einer Gesellschaft bürgerlichen Rechts (GbR, §§ 705 ff. BGB). Zugleich ist das Risiko einer Fusionskontrolle in Deutschland bei marginalen Nettoumsatzerlösen der beteiligten Unternehmen in Anbetracht der deutschen Umsatzschwellen unwahrscheinlich oder gar auszuschließen.

Die Prüfung einer fusionskontrollrechtlichen Anmeldepflicht muss im jeweiligen Einzelfall erfolgen und ist abstrakt anhand des ausdifferenzierten Fusionskartellrechts nicht möglich. Die hier gemachten Ausführungen zur Fusionskontrolle stellen daher einen praktischen Überblick dar, insbesondere mit Blick auf Deutschland. Für eine belastbare Analyse bedarf es im Zweifel des externen Rechtsrats.

2. Mögliche Cyber-Bündnis-Modelle

Im Folgenden werden drei mögliche Cyber-Bündnis-Modelle mit den jeweiligen Vor- und Nachteilen dargestellt. Diese Modelle skizzieren Grundkonzepte und sind keine starren Konstrukte. Die tatsächliche Umsetzung und der Detailgrad der Ausgestaltung kann dem Einzelfall angepasst werden. Zudem sind fließende Übergänge zwischen den Modellen möglich.

Parallel hierzu ist auch eine möglicherweise entstehende Relevanz der kartellrechtlichen Fusionskontrolle stetig zu beachten, welche je nach Entwicklung der Organisationsform und Struktur eines Cyber-Bündnisses bzw. Wabe zwischenzeitlich (ggf. auch wiederholt) einschlägig sein kann. Eine konkrete Bewertung dessen obliegt dem jeweiligen Einzelfall.

2.1 Modell 1: „Handschlag"-Vereinbarung

Das Modell „Handschlag"-Vereinbarung ist dasjenige mit dem geringsten Organisations- und Kooperationsaufwand. Rechtlich gesehen basiert es – je nach konkreter Ausgestaltung im Einzelfall – auf einem reinen Gefälligkeitsverhältnis (ohne Rechtsbindungswillen, § 241 BGB) oder einer Gesellschaft bürgerlichen Rechts (GbR, §§ 705 ff. BGB).

Zusammenfassung

VORTEILE

- zumindest Aussicht auf Hilfeleistung im Notfall und demonstrierte Awareness des Themas Cybersicherheit
- unkompliziert, einfachste „Gründungs"- und Kooperationsform

NACHTEILE

- lockerer Bund mit ggf. rechtlich nicht durchsetzbarer Hilfeleistungs-„Pflicht" (auch im Hinblick auf etwaigen Schadensersatz)
- kaum Verringerung rechtlicher Risiken

BEI GBR: GESELLSCHAFTSRECHTLICHE VORTEILE WIE

- kein Mindest-Stammkapital
- hohes Mitbestimmungsrecht der Gesellschafter
- kaum bürokratischer Aufwand nach der Gründung (Bilanz und Jahresabschluss müssen weder erstellt noch veröffentlicht werden, zumindest bis 60.000 Euro Gewinn bzw. 600.000 Euro Umsatz pro Jahr)

BEI GBR: GESELLSCHAFTSRECHTLICHE NACHTEILE WIE

- Haftung der Gesellschafter mit dem Geschäfts- und Privatvermögen in unbegrenzter Höhe (Haftung mit Privatvermögen nur, wenn es sich um Personengesellschaften bzw. um einen e. K. handelt; falls z. B. eine GmbH Bündnismitglied ist, ist die Haftung grds. begrenzt auf das Gesellschaftsvermögen)
- nur ein lockerer Bund; ohne spezielle Regeln im Gesellschaftsvertrag endet die GbR bereits mit dem Ausscheiden eines Gesellschafters automatisch
- Anwendung des regelmäßigen Einkommenssteuersatzes statt des günstigeren Körperschaftssteuersatzes
- Auch ein Gentleman's Agreement (reiner „Handschlag") ist vom Kartellverbot erfasst.
- Die Vereinbarungen zum Austausch der Mitarbeitenden müssen dann in jedem Einzelfall geprüft werden; insbesondere darf es nicht zum Austausch sensibler Informationen kommen.
- Risiko Fusionskontrolle: Im Falle eines lockeren Zusammenschlusses als reines Gefälligkeitsverhältnis (ohne Rechtsbindungswillen, § 241 BGB) besteht kaum ein Risiko. Dieses erhöht sich mit zunehmender Ausgestaltung des (rechtsverbindlichen) Organisationsmaßes, insbesondere im Falle der Gründung einer GbR.

2.2 Modell 2: „Handschlag plus Standard- und Musterverträge“

Das Modell „Handschlag plus Standard- und Musterverträge“ zeichnet sich durch eine im gewissen Maße verfestigte aber immer noch relativ unaufwändige Organisation aus.

Durch die Verwendung der Musterverträge und -texte ist die Verbindlichkeit und daraus folgende Verlässlichkeit einerseits höher als bei Modell 1, anderseits ist der Organisationsaufwand aber noch vertretbar gering (rechtliche Mindestanforderungen), um den praktischen Anforderungen insbesondere von Kleinstunternehmen hinreichend Rechnung zu tragen. Der Umfang und die Ausgestaltung des Plus an verwendeten Verträgen sind variabel und können den jeweiligen Bedürfnissen des Cyber-Bündnisses entsprechend gewählt werden.

Insgesamt kann durch dieses Modell bereits eine erhebliche rechtliche Risikoverringerung erreicht werden.

Zusammenfassung

VORTEILE

- gewisses Maß an Verbindlichkeit und Verlässlichkeit hinsichtlich Hilfeleistung im Notfall
- unkompliziert, einfache „Gründungs“- und Kooperationsform mit vertretbarem Aufwand insbesondere im Hinblick auf Kleinstunternehmen
- rechtliche Risikoverringerung in wesentlichen Punkten

NACHTEILE

- ggf. aber noch kein ausreichend hohes Maß (oder Höchstmaß) an Verbindlichkeit und Verlässlichkeit hinsichtlich Hilfeleistung
- gewisser organisatorischer Aufwand in der Gründungs- und Betriebsphase
- zwar partielle, aber noch keine vollständige Adressierung rechtlicher Risiken

Bei GbR:

- Je nach Ausgestaltung der Standard- und Musterverträge und der Verbindlichkeit wird kartellrechtlich eher ein Gemeinschafts-unternehmen anzunehmen sein; erforderlich wäre dann eine entsprechende kartellrechtskonforme Ausgestaltung der Verträge einschließlich einer Vertraulichkeitsvereinbarung (diese ist im Übrigen auch wichtig).
- Risiko Fusionskontrolle: Das Risiko erhöht sich mit zunehmender Ausgestaltung des (rechtsverbindlichen) Organisationsmaßes, insbesondere im Falle der Gründung einer GbR. Die Abgrenzung im Rahmen dieses Modells ist ggf. schwierig und extern zu prüfen.

2.3 Modell 3: Organisation in verbindlicher Form (etwa als GmbH)

Das Modell „Eigenständige Cyber-Bündnis Organisation“ zeichnet sich durch eine selbstständige und verbindliche Organisationsstruktur aus. Von den hier vorgestellten drei Modellen hat dieses Modell die komplexeste Organisationsstruktur, die mit einem entsprechend hohen Organisationsaufwand verbunden ist.

Entscheidende Vorteile dieses Modells sind eine „Professionalisierung“ der Sorgfaltspflichten hinsichtlich Cyberrisiken und ein entsprechend hohes Maß an Verbindlichkeit und Verlässlichkeit hinsichtlich Hilfeleistung im Notfall. Rechtliche Risiken können weitgehend adressiert werden. Dementsprechend ist die Cyberrisiko-Compliance am höchsten.

Zusammenfassung

VORTEILE

- hohes Maß an Verbindlichkeit und Verlässlichkeit hinsichtlich Hilfeleistung im Notfall
- weitreichende rechtliche Risikoverringerung in wesentlichen Punkten

gesellschaftsrechtliche/steuerrechtliche Vorteile

- Organisation kann ihren Mitgliedern mehr verbindliche Vorgaben machen, um das Risiko von Kartellrechtsverstößen zu minimieren
- bei Gründung der Organisation ohne Beteiligung großer Unternehmen auch eine fusionskartellrechtliche Anmeldepflicht eher unwahrscheinlich

NACHTEILE

- nicht unerheblicher organisatorischer Aufwand in der Gründungs- und Betriebsphase (Zeit/Geld/Ressourcen)
- Risiko Fusionskontrolle: Nur relevant insbesondere im Falle der erfüllten Aufgreifschwellen. Die Bewertung eines fusionskartellrechtlich relevanten Zusammenschlusses ist abstrakt nicht möglich und vom Einzelfall abhängig.

B. Juristische Aspekte und Rahmenbedingungen

1. IT Compliance und Risk

1.1 Compliance-Verantwortlichkeit für die Schaffung und Erhaltung von Cybersicherheit

Der Einsatz von Informationstechnologie ist aus dem unternehmerischen Alltag längst nicht mehr wegzudenken. Allerdings bringt er auch vielfältige Risiken mit sich, was sich an der weiter erheblich zunehmenden Anzahl von Angriffen zeigt. Solche Risiken bestehen etwa in Angriffen in Netzwerken oder auf Nutzer, in Angriffen auf webbasierte und weitere Anwendungen, auf die Verfügbarkeit, im Einsatz von Schadsoftware sowie in der Datenexfiltration. Unternehmen haben sich deshalb damit zu befassen, wie mit diesen Risiken umzugehen ist.
Fraglich ist zunächst, ob und ggf. auf welchen Rechtsgrundlagen Verantwortlichkeiten im Hinblick auf Fragen der IT-Sicherheit (Begriff nachfolgend verwendet im übergreifenden Sinne unter Einschluss der Informationssicherheit und IT-Sicherheit) bestehen.

1.2 Rechtsgrundlagen

1.2.1 Gesellschaftsrechtlicher Rahmen

Im nicht regulierten Bereich ergeben sich die Verpflichtungen des Managements mit Blick auf die Cybersicherheit aus den allgemeinen Verantwortlichkeits- und Haftungsnormen und den daraus abgeleiteten Legalitäts-, Überwachungs- und Organisationspflichten.

Im Bereich des Aktienrechts finden sich die Grundlagen in den §§ 93, 116 AktG einschließlich § 91 Abs. 2 AktG und auch in § 130 OWiG, wonach zur frühzeitigen Erkennung bestandsgefährdender Entwicklungen geeignete Vorkehrungen, insbesondere ein Überwachungssystem, zu etablieren sind und im Eintrittsfall Gegenmaßnahmen erfordern. Bei GmbHs greift man abgesehen von der allgemein anerkannten „Ausstrahlungswirkung“ dieser Normen auf andere Gesellschaftsformen (vgl. Conrad/Streitz in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutz-recht, 3. Aufl. 2019, § 33 Rn. 40, Thalhofer in Hornung/Schallbruch, IT-Sicherheitsrecht, 2020, S. 371) zurück auf § 43 Abs. 1 GmbHG, für Personengesellschaften werden die §§ 347 HGB, 276 BGB in einer Gesamtschau ergänzend herangezogen. Das Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG) mit seinem originären Ziel der Insolvenzvermeidung bezieht sich darüber hinaus nach § 1 StaRUG explizit und über die aktienrechtlichen Anforderungen hinaus auf alle juristischen Personen. Es erweitert somit den Kreis der Unternehmen, die ein Vorfalls- bzw. Krisenfrüherkennungs- und Krisenmanagementsystem einzuführen haben und im Bedarfsfall geeignete Gegenmaßnahmen einleiten müssen, die ein Fortbestehen des Unternehmens gewährleisten.

Letztlich erfolgt die allgemeine Herleitung der Pflichten damit für alle Gesellschaftsformen aus den Grundsätzen der verantwortungsvollen Leitung der Gesellschaft mit der Sorgfalt einer/s ordentlichen und gewissenhaften Geschäftsleiterin/Geschäftsleiters. Es gehört zu den handels- und gesellschafts-rechtlichen Pflichten jeder Unternehmensleitung, den Bestand des Unternehmens zu sichern und Schäden vom Unterneh-men fernzuhalten (vgl. auch die Grundsätze 4 und 5 des Deutschen Corporate Governance Kodex).

Eine richterliche Konkretisierung des Umfangs dieses Verantwortungsbereichs der Unternehmensleitungen hat das Landgericht München I im Jahr 2013 vorgenommen (LG München I Urt. v. 10.12.2013 – 5 HKO 1387/10). In der sog. Siemens/Neubürger-Entscheidung hat es festgestellt, dass ein Mitglied der Unternehmensleitung im Rahmen seiner Legalitäts- und Legalitätskontrollpflicht dafür Sorge zu tragen hat, dass das Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße erfolgen. Seiner Organisationspflicht genügt ein Vorstandsmitglied bei entsprechender Gefährdungslage nur dann, wenn es eine auf Schadensprävention und Risikokontrolle angelegte Compliance Organisation einrichtet. Entscheidend für den Umfang im Einzelnen sind dabei Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz wie auch Verdachtsfälle aus der Vergangenheit.

Dieses Urteil, das aktuell eine Bekräftigung durch eine rechtskräftige Entscheidung des OLG Nürnberg vom 30.3.2022 (BeckRS 2022, 9637) erfahren hat, wird in der einschlägigen Literatur als auch auf die Aufstellung von Cybersicherheit im Unternehmen übertragbar betrachtet (Conrad/Streitz in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn70 ff.; Thalhofer in Hornung/Schallbruch, IT-Sicherheitsrecht, 2020, S. 370).

Im Kern ist Cybersicherheit damit ein Thema der verantwortlichen Risikovorsorge bzw. des Risikomanagements. Die das Unternehmen oder die Gruppe möglicherweise treffenden Cyberrisiken müssen erkannt, analysiert und behandelt werden. Cybersicherheit umfasst damit letztlich alle Maßnahmen, die zur diesbezüglichen Risikoabwendung bzw. -minimierung abhängig vom bestehenden Risikograd, von der Höhe eines möglichen Schadens sowie von dessen Eintrittswahrscheinlichkeit – und unter den Gesichtspunkten der technischen Machbarkeit und wirtschaftlichen Vertretbarkeit sowie nicht zuletzt im rechtlichen Rahmen – zu treffen sind.

Ein angemessenes Cyber-Risikomanagement gehört also zum Pflichtprogramm jeder sorgfältigen Unternehmensleitung. Mit den entsprechenden organisatorischen Maßnahmen wird die Unternehmensleitung, insbesondere das für Cybersicherheit zuständige Mitglied (das, wie bei allen Risikothemen, das Gremium als solches informiert halten muss), seiner spezifischen Verantwortung gerecht.

Im Hinblick auf die Frage, wie die hiernach bestehende Verantwortung des Managements konkret auszugestalten ist, findet die ebenfalls im gegebenen Kontext anzuwendende Business Judgement Rule (vgl. § 93 Abs. 1 S. 2 AktG) Anwendung. Sie eröffnet Gestaltungsspielräume und entwickelt nötigenfalls eine haftungsprivilegierende Wirkung. Spielräume bestehen indes auch nach Maßgabe von § 91 Abs. 2 AktG und nach herrschender Auffassung auch mit Blick auf die Durchführung der Risikovorsorge. Danach hat die Unternehmensleitung geeignete Maßnahmen zu ergreifen, um den Bestand des Unternehmens gefährdende Entwicklungen frühzeitig zu erkennen. Die für das Unternehmen relevanten IT-Risiken müssen der Unternehmensleitung dabei bekannt sein und zu geeigneten Maßnahmen zur Vermeidung von Cyberrisiken im Unternehmen führen.

Für die weitere Bestimmung des Pflichtenumfangs sind im aufgezeigten Rahmen auch Best Practice-Ansätze wie anerkannte Standards zu berücksichtigen. Relevant sind insoweit jedenfalls die ISO EN 27 000-Reihe und die einschlägigen Ansätze des BSI (BSI-Grundschutz-Kompendium etc.).

Werden die aufgezeigten Pflichten schuldhaft vernachlässigt, kommt eine gesamtschuldnerische sowie persönliche Haftung der Mitglieder der Unternehmensleitung in Betracht. Ein solches Fehlverhalten kann zudem ein wichtiger Grund für die Abberufung oder die fristlose Kündigung des zuständigen Mitglieds der Unternehmensleitung sein.

Auch Cyber-bezogen trifft grundsätzlich alle Mitglieder des Vorstands bzw. der Unternehmensleitung eine Gesamtverantwortung. In diesem Rahmen können indes einzelne Aufgaben wie die Verantwortung für die IT-Systeme und deren Schutz durch Ressortzuweisung an einzelne Mitglieder der Unternehmensleitung und nachgeordnete Personen delegiert werden. Wie im Rahmen allgemeiner Compliance-Strukturen anerkannt, wandelt sich bei einer solchen Delegation die Handlungspflicht in eine Überwachungspflicht. Diese trifft das Gesamtgremium, das nach erfolgter Delegation keineswegs von seiner Verantwortung entbunden ist und dem deshalb Informationsansprüche gegenüber dem Ressortverantwortlichen zustehen.

Bei der Delegation der Pflichten auf andere Unternehmensebenen – wie auch bei der Externalisierung (Cyber-Bündnis) – muss sichergestellt werden, dass die ausgewählte Person bzw. Einheit für die ihr übertragene Aufgabe fachlich qualifiziert und geeignet ist. Dessen hat sich die Unternehmensleitung anfänglich und fortlaufend zu versichern.

1.2.2 Pflichten aus anderen Vorschriften

1.2.2.1 Spezifische Pflichten der KRITIS-Betreiber

Betreiber sog. kritischer Infrastrukturen (KRITIS-Unternehmen; vgl. § 2 Abs. 10 BSIG i.V.m. der sog. KRITIS-Verordnung, die das Bundesinnenministerium gem. § 10 BSIG erlassen hat) haben insbesondere die Pflichten gem. §§ 8a, 8b und 9b BSIG zu erfüllen.

Sie sind explizit verpflichtet, technische und organisatorische Maßnahmen zu ergreifen, um Risiken für die informationstechnischen Systeme, die für die Erbringung ihrer Dienstleistungen oder ihrer Dienste erforderlich sind, abzuwehren. Konkret geht es um die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten und Prozesse unter Berücksichtigung des Standes der Technik. Anerkannte Standards, Regelwerke oder Interpretationsmaßstäbe können die Pflichten konkretisieren und auch den Ermessensrahmen reduzieren. Die technischen und organisatorischen Maßnahmen sind generell dann angemessen, wenn der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder der Beeinträchtigung der betroffenen Infrastruktur steht. Die Unternehmensleitungen haben insoweit eine pflichtgemäße Abwägung der verschiedenen Kriterien wie Aufwand, Eintrittswahrscheinlichkeit und Beeinträchtigungsintensität vorzunehmen.

Die ordnungsgemäße Erfüllung ihrer Pflichten haben KRITIS-Unternehmen gem. § 8a Abs. 3 BSIG alle zwei Jahre gegenüber dem BSI nachweisen, z. B. durch Audits, Zertifikate oder Testate.

1.2.2.2 Pflichten nach der DSGVO

Das Datenschutzrecht bezweckt zwar primär den Schutz natürlicher Personen, nicht der Daten an sich. Dennoch besteht eine unmittelbare Verknüpfung mit der Cybersicherheit. Jeder unberechtigte Zugriff auf die IT-Systeme kann zu einem Verlust oder unberechtigten Zugriff auf personenbezogene Daten führen. Deshalb verpflichten alle Datenschutzgesetze und insbesondere auch die DSGVO die Unternehmen, ihre Systeme gegen einen unbefugten Zugriff oder das Versagen zu schützen, als personenbezogene Daten mit ihnen verarbeitet werden. Art. 25 DSGVO verpflichtet insoweit das verantwortliche Unternehmen zu „geeigneten technischen und organisatorischen Maßnahmen“ zum Datenschutz („TOMs“) und Art. 32 DSGVO verlangt ein „dem Risiko angemessenes Schutzniveau“ bei der Datenverarbeitung, das wiederum durch die TOMs zu gewährleisten ist.

1.3 Compliance-adäquates Vorgehen der Unternehmensleitung(en) zur Prävention mit Blick auf Vorfälle bzw. Angriffe (vor dem Vorfall/Angriff)

Eine verantwortlich handelnde Unternehmensleitung bereitet sich auf – in heutigen Zeiten jederzeit und allerorten – mögliche Vorfälle bzw. Angriffe vor. Die Unternehmensleitung eines jeden Bündnismitglieds muss gewährleisten, dass es über eine Beteiligung an diesem Netzwerk seinen originären Pflichten in angemessenem Umfang nachkommt. Vorgreiflich zu klären ist, ob das Cyber-Bündnis strukturell und in der Organisation geeignet ist, im Beistandsfall Tätigkeiten für das betroffene Unternehmen zu übernehmen, und ob die dort handelnden Personen fachlich qualifiziert und geeignet sind. Dessen hat sich jede Unternehmensleitung eines Bündnismitglieds anfänglich und fortlaufend zu versichern.

1.3.1 Analyse der Cyber-Risk-Exposures

Um den vorstehenden Ansprüchen zu genügen, ist es unerlässlich, zunächst die unternehmensspezifischen Risiken zu erheben. Bei einer Zusammenarbeit im Cyber-Bündnis ist sicherzustellen, dass die Risiken aller Bündnismitglieder angemessen abgebildet werden. Ansonsten werden die Unternehmensleitungen der betreffenden Unternehmen ihrer Verantwortung nicht gerecht. Nach Maßgabe der durchgeführten Risikoanalyse, im Rahmen derer das Cyber-Risk-Exposure ermittelt wird, können Art und Umfang der Schutz- und Hilfsmaßnahmen festgelegt werden. Auch insoweit ist im Cyber-Bündnis sicherzustellen, dass die Maßnahmen einen ausreichenden Schutz und ausreichende Hilfe für alle beteiligten Unternehmen bieten.

Bei der Risikoanalyse sind – rechtlich abgesichert etwa mit Blick auf Aspekte des Geheimnisschutzes und des Wettbewerbsrechts – die IT-Systeme bzw. -Infrastrukturen zu betrachten und die relevanten Daten und Prozesse zu ermitteln, die für das jeweilige Bündnismitglied besonders wichtig sind. Berücksichtigung haben auch Aspekte wie Größe, Branche und Marktstellung des jeweiligen Unternehmens zu finden, denn über sie definiert sich die Frage der Attraktivität des Unternehmens für etwaige Angriffe. Relevant ist auch die Frage, ob es bereits bedeutende und gegebenenfalls sogar erfolgreiche Angriffe auf ein Bündnismitglied gab und insofern erhöhte oder auch geminderte Risiken bestehen.

1.3.2 Risikomanagement

Die identifizierten Risiken sind zu kategorisieren, zu bewerten und sodann in angemessene und effektive Maßnahmen zum Schutz des und der Unternehmen(s) vor Vorfällen bzw. Angriffen zu überführen. Diese Zielsetzung und das entsprechende Vorgehen sind auch im Rahmen des Cyber-Bündnisses zu gewährleisten.

Der gesamte Prozess, von der Bestandsanalyse bis hin zur Entwicklung und Entscheidung technischer und organisatorischer Maßnahmen, ist ausreichend zu dokumentieren, um im Falle von eintretenden kritischen Vorfällen und der Verwirklichung von Schäden die Angemessenheit des Vorgehens und die Einhaltung der erforderlichen Sorgfalt der Unternehmensleitungen belegen zu können. Denn Unternehmen, gegebenenfalls vertreten durch Aufsichtsräte oder Eigentümer, sind gehalten, „eigenverantwortlich das Bestehen von Schadenersatzansprüchen der Gesellschaft gegenüber Vorstandsmitgliedern aus ihrer organschaftlichen Tätigkeit zu prüfen und zu verfolgen" und also Ansprüche aus fehlerhaftem Management geltend zu machen (vgl. ARAG/Garmenbeck-Entscheidung des BGH vom 25.03.1991).

Im Rahmen der Zusammenarbeit im Cyber-Bündnis muss jederzeit gewährleistet sein, dass die zur Prävention mit Blick auf Vorfälle vorgesehenen technischen und organisatorischen Maßnahmen sowie alle weiteren Aktivitäten anforderungskonform mit Blick auf die im einzelnen Unternehmen festgestellte Risikolage sind. Auch dürfen die Maßnahmen nur von sorgsam und nach Maßgabe der Anforderungen ausgewählten Personen intern und beim Cyber-Bündnis durchgeführt werden.

1.3.2.1 Technische Maßnahmen (Überblick)

Präventiv ist unter dem Gesichtspunkt der Verantwortlichkeit zumindest die Sicherstellung dessen erforderlich, dass

- der Virenschutz aller im Unternehmen genutzten technischen Geräte auf aktuellem Stand ist,
- der Virenschutz für die im Unternehmen verwendete Software, vor allem für das Betriebssystem, auf aktuellem Stand ist (Patch-Management),
- der jeweilige Nutzer nach dem Prinzip der minimalen Berechtigungsvergabe nur über die Rechte verfügt, die er zur Ausübung seiner Tätigkeit benötigt (Account-Management),
- sogenannte „starke" (ausreichende komplexe) Passwörter verwendet werden,
- für den Betriebsablauf und das Businessmodell besonders wichtige Daten oder Komponenten von der restlichen IT-Infrastruktur getrennt werden,
- die Backup-Strategie des Unternehmens durch vollständige Offline-Backups ergänzt wird.

1.3.2.2 Organisatorische Maßnahmen (Überblick)

Im Rahmen einer anforderungskonformen Vorbereitung auf Vorfälle bzw. Angriffe müssen zumindest die folgenden Maßnahmen in den Unternehmen sowie – im Rahmen der rechtlichen und faktischen Möglichkeiten – im Cyber-Bündnis ergriffen werden.

Wichtig: Zu berücksichtigen ist, dass es keine Gewähr gibt, dass die Systeme etwa bei einem Angriff noch funktionieren – wichtige Unterlagen sind deshalb ausgedruckt vorzuhalten.

- Inventarisierung der vorhandenen IT-Infrastruktur (Hardware, Software, interne und externe Netzwerkverbindungen, Auslastungen, Schutzvorrichtungen etc.),
- Festlegung von Verantwortlichkeiten und Schnittstellen (Organisationsplan, namentliche Benennung von Personen und Funktionen, Weisungs- und Kontrollstrukturen etc.),
- Klärung von Befugnissen,
- Berichtspflichten, Berichtswege, Berichtszeitpunkte,
- Einrichtung Meldestelle(n) für Vorfälle bzw. Angriffe, Hotline, Koordinationsstelle innerhalb des Cyber-Bündnisses,
- Notfallplan, Cyber Incident Response Plan (CIRP),
  - Defintion der Art von Vorfällen bzw. Angriffen,
  - Festlegung, auf welche Arten von Vorfällen bzw. Angriffen in welcher Art und auf welche Weise reagiert werden soll,
  - Festlegung Verantwortlichkeiten, Benennung (konkreter) Ansprechpartner, Aufgaben und Kompetenzen,
- Bildung Task Force/Krisenstab im Unternehmen (Cyber Response Team (insb.: Unternehmensleitung(en), Einheiten Recht, Compliance, IT, CISO, DSB, BR, Externe und übergreifend im Cyber-Bündnis)),
- Vorbereitung Kommunikation (ggf. einheitlich im Cyber-Bündnis),
  - Zuständigkeit für Kommunikation,
  - Stakeholder,
  - Erarbeitung Texte unter Berücksichtigung denkbarer Szenarien,
  - Kommunikationskonzept: Ausgangslage, Zielgruppen, kommunikative Ziele, Inhalte, Umfang, Transparenz, Kommunikationskanäle,
  - Basis-Q&A,
- Abstimmungen zu Fragen des Cyber-Versicherungsschutzes im Cyber-Bündnis, Klärung von Auswirkungen auf das Einzelunternehmen,
- Vorbereitung Einbindung staatliche Stellen,
- Vorbereitung Hinzuziehung IT-Forensik,
- Vorbereitung Einbindung spezialisierter Berater, etwa bei Fällen von Erpressung (Organisation des Zugriffs auf Bitcoins wegen etwaiger Lösegeldforderungen o. ä., aber rechtlich problematisch, siehe unten),
- Erarbeitung spezifischer Richtlinien und Handlungsanweisungen,
- Awareness-Schulungen und Übungen für Mitarbeitende, auch im gesamten Cyber-Bündnis,

- Vorabklärung des Sonderthemas „Lösegeldforderungen“:
  - BSI und BKA raten von Lösegeldzahlungen ab, da Bestärkung Krimineller, weitere Cyberangriffe durchzuführen,
  - Ungewissheit, ob betroffene Systeme oder Daten tatsächlich freigeschaltet werden,
  - Rechtlich: Gefahr, dass in der Zahlung die Unterstützung einer (ausländischen) kriminellen Vereinigung gem. §§ 129 Abs. 1 S. 2, 129 b Abs. 1 StGB gesehen wird (mindestens Abstimmung mit der zuständigen Staatsanwaltschaft, auch bzgl. etwaiger Rechtfertigungstatbestände wie Notstand (§ 34 StGB)).

1.4 Compliance-adäquates Vorgehen der Unternehmensleitungen im Falle eines Vorfalls bzw. Angriffs (während und nach dem Vorfall/Angriff)

Kommt es zu einem Vorfall bzw. Angriff, verdichten sich die Handlungspflichten insbesondere der unmittelbar zuständigen Ressortverantwortlichen der Bündnismitglieder und auch die Überwachungspflichten der jeweiligen Unternehmensleitungen. Dies gilt auch bereits bei bloßen Verdachtsmomenten, schon dann sind unverzüglich alle erforderlichen Maßnahmen auf Unternehmensebene zu ergreifen, um das Schadensrisiko zu begrenzen. Die Unternehmensleitungen haben angemessen zu reagieren, auch in zeitlicher Hinsicht.

Seitens des Cyber-Bündnisses (je nach Organisationsform bzw. Verselbstständigung und konkreter Ausgestaltung) ist den ihm insoweit übertragenen Aufgaben vollumfänglich nachzukommen. Die Beauftragung hat in eindeutiger Weise und inhaltlich nachvollziehbar sowie dokumentiert zu erfolgen. Alle Tätigkeiten im Cyber-Bündnis sind seitens der betroffenen Unternehmen durch eine enge und fortlaufende Überwachung der dort ergriffenen Maßnahmen und seitens des Cyber-Bündnisses durch ein entsprechendes Reporting zu begleiten und zu unterstützen.

Etwaig vor dem Hintergrund des Vorfalls bzw. Angriffs erkannte Defizite in der Aufstellung der betroffenen Unternehmen sind durch entsprechende Maßnahmen im Bereich des oder der jeweiligen Unternehmen(s) unverzüglich zu beheben. Das Cyber-Bündnis ist im Rahmen des rechtlich Zulässigen zu informieren, um eine Optimierung auch von dessen Aufstellung zu erreichen.

Ein anforderungskonformer Umgang mit einem akuten Vorfall bzw. Angriff erfordert mindestens das unverzügliche Ergreifen der nachfolgend dargestellten Maßnahmen durch das Cyber-Bündnis bzw. die Bündnismitglieder.

1.4.1 Erfassung und Bewertung des Vorfalls

Im Falle eines Vorfalls ist die betroffene Unternehmensleitung wie aufgezeigt verpflichtet, angemessen zu reagieren. Sie hat unverzüglich die Lage zu analysieren und festzustellen, ob und wenn ja, welche Art eines Vorfalls vorliegt und welche Geschäftsbereiche, Systeme und Daten betroffen sind. Das Cyber-Bündnis ist bzw. dessen Mitglieder sind über die für dessen Tätigkeit relevanten Umstände – im Rahmen der rechtlichen Möglichkeiten – zu informieren, um zur Hilfeleistung in der Lage zu sein.

Die Analyse ermöglicht die vom betroffenen Unternehmen vorzunehmende Bewertung, ob gesetzliche Meldepflichten etwa mit Blick auf den Kapitalmarkt oder nach Maßgabe der DSGVO (Art. 33, 34 DSGVO) zu erfüllen sind (Achtung: Hier stehen weitere Meldepflichten an das BSI nach dem zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme im Raum).

Ferner kann das Unternehmen auf der Grundlage der Bewertung zusammen mit dem Cyber-Bündnis über technische Abwehr- und Wiederherstellungsmaßnahmen beraten und Maßnahmen ergreifen. Das Letztentscheidungsrecht insoweit verbleibt stets bei dem betroffenen Unternehmen.

1.4.2 Vorfalls- und Krisenmanagement

Während und nach einem Vorfall bzw. einer Krise ist unter dem Gesichtspunkt der Verantwortlichkeit im betroffenen Unternehmen zumindest die Durchführung folgender Maßnahmen erforderlich. Das Cyber-Bündnis empfiehlt die Maßnahmen und unterstützt umfassend bei deren Umsetzung. Die Letztverantwortung und das Letztentscheidungsrecht stehen aber dem betroffenen Unternehmen zu.

1.4.2.1 Technische Maßnahmen

Folgende technischen Maßnahmen sind essenziell im Umgang mit Vorfällen, insbesondere Angriffen, und daher zwingend zu ergreifen:

- Beweissicherung (IT-Forensik),
  - Zum Schutz vor etwaigen Forderungen Dritter und wegen der Regulierung etwaiger Schäden,
  - Gefahr des Verlustes von Beweismöglichkeiten bei zu früher Wiederherstellung des Systems – Abwägung jur./techn. zur schnellen Identifikation der Beweise mit einer relevanten Bedeutung und zur Dokumentation,
  - Sicherungen, z. B. Logfiles, Notizen oder Screenshots,
- Zur Wiederherstellung des Betriebsablaufs,
  - Trennung des betroffenen Systems vom Unternehmensnetzwerk und ggf. auch vom Internet,

– Stoppen von laufenden Back-ups,
– Schutz integrer Back-ups vor einem Kontakt mit dem infizierten System.

1.4.2.2 Organisatorische Maßnahmen

Folgende organisatorische Maßnahmen sind essenziell im Umgang mit Vorfällen, insbesondere Angriffen, und daher zwingend und unverzüglich vom betroffenen Unternehmen unter seiner Verantwortung gemeinsam mit dem Cyber-Bündnis zu ergreifen:

- Information der im Unternehmen und im Cyber-Bündnis zuständigen Stellen,
- Einberufung interne Task Force/interner Krisenstab und Cyber-Bündnis,
- Durchführung aller im Notfallplan geregelten Schritte, insbes. Maßnahmen zur Schadensbegrenzung,
- Protokolle, Dokumentation des Gesamtverfahrens (ausreichend für Beweiszwecke für Zwecke der Rechtsverfolgung und mit Blick auf Einhaltung Sorgfaltserfordernisse, z. B. konkret ergriffene Handlungen, tätige Personen, jeweilige Zeitpunkte unter Angabe des Datums und der Uhrzeit, Telefonate, Mails etc.),
- Dokumentation der betroffenen Systeme, Dienste, Konten, Daten und Netze sowie die Art der Beeinträchtigung,
- Externe (ggf. Öffentlichkeit) und interne Kommunikation nach Maßgabe der aufgestellten Leitlinien (s. o. – nicht über das infizierte System, Nutzung alternativer Wege),
- Einholung von Rechtsrat,
- Einbindung der Ermittlungsbehörden bei Verdacht einer Straftat (Polizei und Staatsanwaltschaft mit spezifisch zuständigen Stellen),
- Unverzügliche Meldung an Versicherung,
- Ggf. unverzügliche Kapitalmarktmeldung (ad hoc-Meldepflichten für kapitalmarkorientierte Unternehmen),
- Ggf. unverzügliche Einbindung der Datenschutzaufsicht und der Betroffenen (Verlust von Kundendaten o. ä.) und weiterer Behörden,
- Sonderthema: Lösegeldforderungen (auch rechtlich problematisch, s. o.).

1.4.3 Vorgehen nach dem Vorfall

Nach einem Vorfall sind die entsprechenden Schlussfolgerungen zu ziehen („Lessons Learned“) und erkannte organisatorische oder prozessuale Schwachstellen im System zu schließen.

Gegebenenfalls ist der Notfallplan unter Berücksichtigung der gewonnenen Erkenntnisse und ergriffenen Maßnahmen anzupassen. Alle Maßnahmen sind zu dokumentieren und aus Compliance-Sicht unter Einbezug der im Unternehmen verantwortlichen Stellen zu bewerten.

2. Mitgliedschaft im Cyber-Bündnis als Compliance-Maßnahme

Das Cyber-Bündnis orientiert sich in seiner Aufstellung an Best Practice-Ansätzen nach Maßgabe anerkannter Standards. Insoweit also den Anforderungen an ein Compliance-adäquates Vorgehen in allen relevanten Phasen Rechnung getragen wird (s. o. Ziff. 1.2. und 1.3.), ist mit Blick auf das Cyber-Bündnis grundsätzlich davon auszugehen, dass eine Teilnahme an diesem eine geeignete Compliance-Maßnahme mit Blick auf die Risiken aus Vorfällen bzw. Angriffen darstellt. Sie führt dazu, dass das Management eines Bündnismitglieds seiner Verantwortung mit Blick auf Cyberrisiken gerecht wird.

Das Management des Bündnismitglieds ist grundsätzlich frei in der Entscheidung darüber, wie es den relevanten unternehmensspezifisch identifizierten IT-Risiken begegnet (s. o. Ziff. 1.1.). Bei einer – bezogen auf das Cyber-Bündnis gegebenen – Externalisierung von Pflichten muss indes, wie bei einer Delegation auf andere Unternehmensebenen, stets sichergestellt werden, dass die ausgewählte Einheit und die dort handelnden Personen für die ihr übertragene Aufgabe fachlich qualifiziert und geeignet sind. Dessen hat sich die delegierende Unternehmensleitung daher auch im Falle der Mitwirkung in einem Cyber-Bündnis anfänglich und fortlaufend zu versichern. Wie im Rahmen allgemeiner Compliance-Strukturen anerkannt, wandelt sich bei einer solchen Delegation die Handlungspflicht in eine Überwachungspflicht. Das jeweilige Management hat die Funktionsfähigkeit des Cyber-Bündnisses also regelmäßig und, bei entsprechenden Anhaltspunkten, auch ad hoc zu überprüfen.

Auch nach einem erfolgten Beitritt zu einem Cyber-Bündnis bedarf es überdies stets einer Aktualität des unternehmensspezifischen IT-Risikoprofils und eines laufenden Abgleichs mit dem Leistungsprofil des Cyber-Bündnisses.

Die damit grundsätzlich angemessene Compliance-Maßnahme der Mitwirkung in einem Cyber-Bündnis ist ferner an den allgemeinen Anforderungen für Managemententscheidungen zu messen:

- Im Verhältnis zu einem individuellen Vorhalten der kompletten Struktur zur Herstellung von Cyber-Resilienz in jedem einzelnen Unternehmen ist der Cyber-Bündnis-Ansatz eine – bei voraussichtlich gleicher Wirksamkeit (Business Judgement Rule) – ressourcenschonendere Vorgehensweise. Sie steht damit im unternehmerischen Interesse.
- Sicherzustellen ist zudem, dass seitens des einzelnen Bündnismitglieds eine Kompatibilität der Prozesse im Cyber-Bündnis mit den unternehmensinternen Prozessen besteht. Insbesondere angewandte Techniken müssen getestet und als wirksam abgenommen werden. Auch wenn Effizienzgründe bei der Mitwirkung im Cyber-Bündnis maßgeblich sind, muss die spezifische Unternehmensorganisation in enger Verzahnung mit dem Cyber-Bündnis handlungsfähig sein. Entsprechendes gilt mit Blick auf die internen personellen Ressourcen, die mit ausreichender fachlicher Kompetenz an der Schnittstelle zum Cyber-Bündnis stehen.

3. Arbeitsrecht

Im Folgenden werden die aus arbeitsrechtlicher Sicht relevanten Gesichtspunkte in der gebotenen Kürze dargestellt.

3.1 Arbeitszeit

Die Vorgaben des Arbeitszeitgesetzes und andere Arbeitnehmerschutzgesetze gelten auch während eines Vorfalls bzw. einer Krise; d. h., dass etwa die Regelungen zur täglichen und wöchentlichen Höchstarbeitszeit, zu Mindestpausen, zum Verbot von Sonn- und Feiertagsarbeit, zur Mindestruhezeit zwischen zwei Arbeitseinsätzen grundsätzlich beachtet werden müssen.

Bei **kritischen Vorfällen**, etwa dem drohenden Verlust von erheblichen Arbeitsergebnissen oder Ähnlichem sind Ausnahmen nach § 14 Arbeitszeitgesetz möglich. Verstöße sind grundsätzlich strafbar, ebenso die Fehleinschätzung über das Vorliegen eines Notfalls. Im Zweifel daher vor Nichtbeachtung der Vorgaben des Arbeitszeitgesetzes einen Fachanwalt für Arbeitsrecht um eine Stellungnahme ersuchen, ob ein kritischer Vorfall bzw. arbeitsrechtlicher „Notfall" vorliegt. Wenn der Anwalt sich täuscht, haftet er.

3.2 Arbeitnehmerdatenschutz

Bei jedem Einsatz ist es hochwahrscheinlich, dass personenbezogene Daten von Arbeitnehmenden/Kunden/Lieferanten des angegriffenen Unternehmens dritten Helfenden zugänglich werden. Hierfür braucht man eine rechtliche Grundlage, die im Hinblick auf Arbeitnehmende durch entsprechende Betriebsvereinbarungen geschaffen werden kann (siehe die verschiedenen **Muster-Betriebsvereinbarungen** auf der Website), wenn es einen Betriebsrat im betroffenen Unternehmen gibt.

Auch im Übrigen dürfen personenbezogene Daten nur unter Beachtung der datenschutzrechtlichen Grundsätze aus Art. 5 DSGVO (vertiefend hierzu unter Ziff. 5 zum allgemeinen Datenschutz) verarbeitet werden. Hervorzuheben ist der Zweckbindungsgrundsatz: Demnach ist jede Verarbeitung personenbezogener Daten, die für die Hilfeleistung nicht erforderlich ist, strikt untersagt. Insbesondere unzulässig wäre es beispielsweise, wenn Hilfe leistende Mitarbeiter Kunden- oder Lieferantendaten eines betroffenen Unternehmens in das eigene Unternehmen mitnehmen, um diese Daten zu anderen als zur Hilfeleistung erforderlichen Zwecken zu verarbeiten, z. B. um damit eigenes Geschäft zu akquirieren. Dies wäre auch unter dem Gesichtspunkt der Vertraulichkeit und des Schutzes von Betriebs- und Geschäftsgeheimnissen (vgl. **Muster-Vertraulichkeitsvereinbarung** auf der Website) unzulässig.

3.3 Arbeitnehmerhaftung

Für die Arbeitnehmerhaftung im Arbeitsverhältnis gilt der Grundsatz des so genannten innerbetrieblichen Schadensausgleichs, der verschiedene Privilegierungen der Arbeitnehmer vorsieht. Dieser ist im Einzelnen recht komplex und soll daher nachfolgend nur vereinfacht in Grundzügen dargestellt werden: Arbeitnehmer haften bei Vermögensschäden und Sachschäden nach den Grundsätzen des innerbetrieblichen Schadensausgleichs nicht, wenn sie leicht fahrlässig handeln, sie haften nur anteilig bei mittlerer Fahrlässigkeit, bei grober Fahrlässigkeit und Vorsatz haften sie uneingeschränkt.

Grob fahrlässig handelt ein Arbeitnehmer dann, wenn er diejenige Sorgfalt außer Acht gelassen hat, die jedem eingeleuchtet hätte (Beispiel: Überfahren einer roten Ampel mit dem Dienstwagen und dadurch Verursachen eines Verkehrsunfalls).

Mittlere Fahrlässigkeit bewegt sich zwischen leichter und grober Fahrlässigkeit und liegt dann vor, wenn der Arbeitnehmer die erforderliche Sorgfalt außer Acht gelassen hat, er hat also in Kauf genommen, dass etwas zu Schaden kommen könnte, hält es aber nicht für wahrscheinlich (Beispiel: Abstellen eines LKW auf einer leicht abschüssigen Fläche ohne Anziehen der Handbremse). Ihm sind aber keine schweren Vorwürfe zu machen.

Handelt es sich lediglich um ein unerhebliches Fehlverhalten des Arbeitnehmers, liegt also nur eine kurze Unachtsamkeit vor, handelt es sich lediglich um leichte Fahrlässigkeit (Beispiel: Verschütten eines Getränkes auf der Tastatur).

Bei einer anteiligen Haftung des Arbeitnehmers infolge einer mittleren Fahrlässigkeit erfolgt eine Quotelung des Schadens. Diese erfolgt nicht automatisch hälftig, sondern ist stets einzelfallabhängig und richtet sich nach verschiedenen Faktoren, wie bspw. der Gefahrgeneigtheit der Tätigkeit, der Höhe des Schadens im Verhältnis zum Einkommen, dem Vorverhalten des Arbeitnehmers etc.

Die schuldhafte Schädigung von außenstehenden Dritten wie z. B. Kunden, oder hier eines Mitgliedsunternehmens des Cyber-Bündnisses bei der Arbeitsleistung, verpflichtet den Arbeitnehmer im Außenverhältnis zum Schadensersatz. Soweit er aber nach den Grundsätzen des innerbetrieblichen Schadensausgleichs nicht haften würde, hat er einen Freistellungsanspruch gegen den Arbeitgeber, hier also gegen das helfende Unternehmen. Zu überlegen ist, inwieweit sich die Mitgliedsunternehmen nicht wechselseitig von einer möglichen Haftung durch Fehler der helfenden Fremdarbeitnehmer freistellen. Das heißt, die Mitgliedsunternehmen treffen eine Vereinbarung, wonach die Unternehmen jeweils die Haftung für bei ihnen eingesetzte Fremdarbeitnehmer übernehmen und damit das helfende Unternehmen von möglichen Haftungsansprüchen freistellen. Hierfür könnte das unter-

stützte Unternehmen gegenüber dem helfenden Unternehmen schriftlich erklären, dass es dieses von jeglichen Haftungsansprüchen aus innerbetrieblichem Schadensausgleich im Zusammenhang mit Handlungen des helfenden Fremdarbeitnehmers freistellt.

3.4 Hilfseinsatz remote

Bei einem Hilfseinsatz remote stellen sich grundsätzlich keine großen arbeitsrechtlichen Probleme, solange die Mitarbeitenden nicht Weisungen im betroffenen Betrieb erteilen oder solche Weisungen erhalten.

Wenn der Hilfseinsatz länger dauert oder völlig andere Arbeitsinhalte verlangt als die normale Tätigkeit, kann kollektivrechtlich eine Versetzung vorliegen, diese unterliegt dem Mitbestimmungsrecht des Betriebsrats des Arbeitgebers. Gleiches gilt für eine geänderte Lage oder Länge der Arbeitszeit in einem solchen Fall. Für diese Konstellationen kann eine Betriebsvereinbarung über einen Vorfall hilfreich sein (siehe die verschiedenen **Muster-Betriebsvereinbarungen** auf der Website).

Weiter ist darauf zu achten, dass arbeitsvertraglich solche Einsätze vom Direktionsrecht umfasst werden (siehe die **Musterklauseln Arbeitsvertrag** auf der Website).

3.5 Hilfseinsatz vor Ort beim betroffenen Unternehmen

3.5.1 Individualarbeitsrechtlich

Zunächst stellt sich die Frage: Wie bekomme ich die Helfenden zum betroffenen Unternehmen? Es gibt rechtlich im Regelfall kein Weisungsrecht beim Dritten zu arbeiten. Wenn dieser weisungsberechtigt sein soll, dann gegebenenfalls also nur Freiwillige.

Besser aber: Darauf achten, dass vom betroffenen Unternehmen gegenüber Helfenden keine – allenfalls fachliche – Weisungen erteilt werden, keinesfalls disziplinarische, da ansonsten individualrechtlich eine Einstellung beim betroffenen Unternehmen vorliegen könnte und es zu Problemen mit dem Arbeitnehmerüberlassungsgesetz kommt. Am besten mit einem Einsatzleiter des helfenden Unternehmens für alle Helfer des helfenden Unternehmens arbeiten, der die klassischen Weisungen (wann, wo, was, wie) im bestehenden Arbeitsverhältnis erteilt. Voraussetzung für eine solche „Entsendung" zum betroffenen Unternehmen ist die Vereinbarung eines entsprechend weiten Weisungsrechts in örtlicher Hinsicht im Arbeitsvertrag (siehe die **Musterklauseln Arbeitsvertrag** auf der Website).

3.5.2 Kollektivrechtlich (nur wenn ein Betriebsrat besteht)

Fremdfirmenkräfte, die bei einer Cyber-Attacke im angegriffenen Unternehmen helfen, lösen je nach Ausgestaltung beim aufnehmenden Betrieb Mitbestimmungsrechte nach § 99 BetrVG (Einstellung) aus, insbesondere, wenn typische Weisungen (was, wann, wie, wo) vom aufnehmenden Betrieb erfolgen – ggf. Regeln dazu via Cyber-Betriebsvereinbarung (siehe die verschiedenen **Muster-Betriebsvereinbarungen** auf der Website). Best Practice ist auch hier ein verantwortlicher Einsatzleiter für alle (disziplinarischen) Weisungen vom helfenden Unternehmen für dessen Helfer.

Im „abgebenden Betrieb" liegt kollektivrechtlich sehr wahrscheinlich eine Versetzung vor; das Verfahren hierzu kann in einer in Betriebsvereinbarung „Vorfall" geregelt werden (siehe die verschiedenen **Muster-Betriebsvereinbarungen** auf der Website).

Alternative bei nicht kooperierendem Betriebsrat ist das Vorgehen nach § 100 BetrVG („vorläufige personelle Maßnahme"). Bestreitet der Betriebsrat das Vorliegen der „sachlichen Dringlichkeit, so muss ein Antrag bei Gericht gestellt werden, der sich aber im Regelfall aufgrund der zeitlichen Begrenztheit des Einsatzes der Mitarbeitenden beim betroffenen Unternehmen vor einer Entscheidung des Gerichts erledigen wird.

Je nach Art der Hilfe kann auch Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen" bestehen, dies gilt auch beim Remote-Einsatz (s. o. unter Ziff. 3.4). Auch hier hilft eine Betriebsvereinbarung „Vorfall" (siehe die verschiedenen **Muster-Betriebsvereinbarungen** auf der Website).

4. Kartellrecht

4.1 Ziele und Regelungen des Kartellrechts (Überblick)

Das Kartellrecht beruht auf den drei Säulen Kartellverbot, Missbrauchs- und Fusionskontrolle.

4.1.1 Kartellverbot

Das deutsche und europäische Kartellrecht verbieten Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, die eine Verhinderung, Einschränkung oder Verfälschung[1] des Wettbewerbs bezwecken oder auch nur (spürbar) bewirken (Art. 101 AEUV, § 1 GWB).

[1] Oberbegriff ist die Wettbewerbsbeschränkung.

Dieses Verbot gilt sowohl für Vereinbarungen zwischen Unternehmen auf demselben Markt und derselben Marktstufe, d. h. tatsächlichen oder jedenfalls potenziellen Wettbewerbern, ob als Anbieter oder Nachfrager (horizontale Beschränkungen), als auch für Vereinbarungen zwischen Marktteilnehmern auf verschiedenen Ebenen der Produktions- oder Vertriebskette (vertikale Beschränkungen).

Der Anwendungsbereich des Kartellverbots ist weit gefasst und wird durch die Entscheidungspraxis und Veröffentlichungen der Wettbewerbsbehörden sowie die Rechtsprechung weiter präzisiert. Daher ist in der Regel eine Einzelfallprüfung erforderlich, ob eine Wettbewerbsbeschränkung vorliegt.

Der Begriff der „Vereinbarung" erfasst nicht etwa nur Verträge, sondern auch rein faktische Vereinbarungen. Sie müssen nicht rechtsverbindlich sein. Auch die Form ist unerheblich. Es werden sowohl mündliche oder schriftliche, formelle oder informelle, implizite oder explizite Vereinbarungen umfasst.[2] Bereits der Abschluss einer Vereinbarung als solcher ist verboten, auch wenn sie nicht in die Tat umgesetzt wird.

Unabhängig davon ist die Frage zu sehen, welche Verbindlichkeit die Kooperation im Rahmen der getroffenen Vereinbarung hat. So sind etwa Einkaufsgemeinschaften (unter weiteren Voraussetzungen) eher dann zulässig, wenn sie die Mitglieder nicht exklusiv verpflichten.

Neben einer wettbewerbsbeschränkenden Vereinbarung fallen auch abgestimmte Verhaltensweisen unter das Kartellverbot des Art. 101 Abs. 1 AEUV respektive § 1 GWB. Darunter fällt u. U. auch der Informationsaustausch bezüglich wettbewerblich relevanter Informationen. Die Kartellbehörden gehen davon aus, dass ein solcher Austausch regelmäßig zu einem abgestimmten Verhalten führt.

Eine Wettbewerbsbeschränkung wird bereits auf Tatbestandsebene ausgeschlossen, wenn eine sogenannte Arbeitsgemeinschaft vorliegt. Der Arbeitsgemeinschaftsgedanke schließt eine Wettbewerbsbeschränkung aus, soweit die Beteiligten im konkreten Fall nicht im Wettbewerb stehen, entweder, weil sie allein nicht über die erforderliche Kapazität zur Bedienung einer Anfrage verfügen, oder zwar die erforderliche Kapazität haben, aber erst die Arbeitsgemeinschaft sie in die Lage versetzt, ein wirtschaftliches Angebot abzugeben.

Liegt eine Wettbewerbsbeschränkung vor, gibt es die Möglichkeit der Freistellung und zwar auf Grundlage einer sog. Gruppenfreistellungsverordnung oder im Wege der Einzelfreistellung. Im Falle kleinerer und mittlerer Unternehmen („KMUs") kommt darüber hinaus eine Privilegierung gem. § 3 GWB[3] in Betracht.

[2] Sogar „Frühstückskartelle", d. h. (regelmäßige) Frühstücksrunden unter Konkurrenten, bzw. sog. „Gentlemen's Agreements" sind erfasst.
[3] Vgl. auch für weitere Konkretisierungen: Merkblatt des Bundeskartellamtes über Kooperationsmöglichkeiten für kleinere und mittlere Unternehmen.

Die Gruppenfreistellungsverordnungen (GVO) der EU-Kommission sind auch im nationalen deutschen Kartellrecht anwendbar, § 22 Abs. 2 S. 1 Nr. 3 GWB. In den Gruppenfreistellungsverordnungen sind im Grundsatz ganz bestimmte Arten von Vereinbarungen unterhalb bestimmter Marktanteilsschwellen generell freigestellt, sofern keine Kern-Beschränkung vereinbart ist.

Daneben kommt auch je nach den konkreten Umständen eine Einzelfreistellung nach Art. 101 Abs. 3 AEUV respektive § 2 GWB in Betracht. Dafür müssen die Effizienzvorteile einer Absprache oder abgestimmten Verhaltensweise die negativen Auswirkungen auf den Wettbewerb überwiegen. Ob diese Voraussetzungen gegeben sind, müssen die handelnden Unternehmen selbst prüfen.

Eine Leitlinie für einen bestimmten Fall enthält § 3 GWB, wonach Vereinbarungen oder aufeinander abgestimmte Verhaltensweisen zur Rationalisierung zwischen kleinen und mittleren Unternehmen gem. § 2 Abs. 1 GWB freigestellt sind. Der Begriff des kleinen oder mittleren Unternehmens ist hierbei relativ zu verstehen; es kommt auf die Größe des jeweiligen Unternehmens auf dem relevanten Markt an. Das Cyber-Bündnis wird bzw. dessen Mitglieder werden auf dem Markt für IT-Dienstleistungen, insbesondere Unterstützung bei einem Vorfall bzw. einer Krise, tätig werden. Das ist der relevante Markt. Hier dürften die meisten Bündnismitglieder im Verhältnis kleine oder mittlere Unternehmen darstellen. Mithin ist die Wahrscheinlichkeit einer Privilegierung nach § 3 GWB für das Cyber-Bündnis insofern erhöht.

Nach diesen Grundsätzen ist eine Zusammenarbeit zwischen den Bündnismitgliedern grundsätzlich dann eher problematisch, wenn sie zwischen tatsächlichen oder potenziellen Wettbewerbern erfolgt, und spiegelbildlich dann eher unproblematisch, wenn die Beteiligten nicht zueinander im Wettbewerb stehen. Des Weiteren ist mit Blick auf bewirkte Wettbewerbsbeschränkungen die angedachte Wabenstruktur vorteilhaft, insbesondere bei Waben, in denen KMUs organisiert sind. Denn solche Kooperationen haben möglicherweise keine spürbaren Effekte und können darüber hinaus selbst bei Vorliegen einer spürbaren Wettbewerbsbeschränkung auch und gerade im Falle von kooperierenden Wettbewerbern gem. §§ 2, 3 GWB unter weiteren Voraussetzungen kartellrechtlich freigestellt sein. Schließlich sind unverbindliche Goodwill-Erklärungen wettbewerbsrechtlich grundsätzlich unproblematischer als verbindliche, evtl. sogar exklusive Verpflichtungen.

4.1.2 Verbot des Missbrauchs von Marktmacht

Das Kartellrecht verbietet den Missbrauch von (relativer) Marktmacht (Art. 102 AEUV, §§ 18 ff. GWB). Die Bewertung der (relativen, überlegenen oder großen) Marktmacht eines Unternehmens bedarf einer Gesamtschau der Umstände des Einzelfalles, wobei bei einem Marktanteil von mind. 40 % auf dem sachlich, räumlich und (dem u. U. ebenfalls zu bestimmenden) zeitlich relevanten Markt eine

marktbeherrschende Stellung vermutet wird (vgl. § 18 Abs. 4 GWB). Für die Bestimmung der Marktstellung eines Unternehmens hat der deutsche Gesetzgeber zahlreiche beispielhafte, nicht abschließende Kriterien benannt, vgl. §§ 18 und 20 GWB. Der relevante Markt ist hier jedenfalls der für die Nachfrage von IT-Dienstleistungen, auf dem die Bündnismitglieder jeweils als auch in ihrer Gesamtheit keine Marktmacht haben dürften. Das Missbrauchsverbot wird daher in den weiteren Ausführungen ausgeklammert.

4.1.3 Fusionskontrolle

Zusammenschlüsse von Unternehmen unterliegen unter bestimmten Voraussetzungen der Fusionskontrolle in einem oder gar mehreren Ländern. In diesem Falle sind sie bei der entsprechend zuständigen staatlichen Stelle eines Landes (in Deutschland das Bundeskartellamt) anzumelden und dürfen in der Regel nicht ohne dessen Freigabe vollzogen werden. Zweck dieser Kontrolle ist der Schutz vor wesentlicher Beeinträchtigung des strukturellen Wettbewerbs im Wege der übermäßigen Konzentration von Marktmacht durch externes Wachstum.

Fusionskontrollrecht besteht als nationales Recht in zahlreichen Ländern (insbesondere in nahezu allen EU-Mitgliedsstaaten) sowie auf supranationaler Ebene (insbesondere der Europäischen Union mit der Europäischen Kommission als zuständige Behörde). Die Notwendigkeit und der Umfang einer Fusionskontrolle in einem Land bzw. Jurisdiktion richten sich nach dem jeweils anwendbaren nationalen oder supranationalen Recht, wobei zwischen den Rechtsordnungen ganz erhebliche Unterschiede bestehen können.

Der Fusionskontrolle können insbesondere auch – unabhängig von der gewählten Rechtsform – Joint Ventures unterliegen. Ferner können unter Umständen deutsche Unternehmen (insbesondere aufgrund ihrer ausländischen Geschäftsaktivitäten sowie -verbindungen) bei einem Zusammenschlussvorhaben in Deutschland einer Anmeldepflicht im Ausland unterliegen.

Näheres zu der Relevanz der Fusionskontrolle im Rahmen des Cyber-Bündnisses wird im Abschnitt „Organisation“ erläutert.

4.2 Haftung bei Kartellrechtsverstößen

Die Nichteinhaltung des Kartellrechts kann schwerwiegende Folgen nach sich ziehen. Das eine Risiko sind Geldbußen, welche in Höhe von bis zu 10 % des Konzernumsatzes des betreffenden Unternehmens im letzten abgeschlossenen Geschäftsjahr auferlegt werden können. Die konkrete Höhe der Geldbuße hängt von den Umständen im Einzelfall ab, insbesondere der Schwere und Dauer des jewei-

ligen Verstoßes. Grundsätzlich sind die betroffenen Unternehmen selbst haftbar, doch sehen mehrere nationale Wettbewerbsgesetze (wie auch in Deutschland) eine individuelle Haftung der handelnden Personen vor.

Darüber hinaus sind Vereinbarungen, die gegen Kartellrecht verstoßen, automatisch nichtig. Dies betrifft, je nach nationalem Recht, nur die kartellrechtswidrige Bestimmung oder die Vereinbarung im Ganzen.

Ein Verstoß birgt u. U. auch das Risiko von Schadenersatzansprüchen derjenigen, die durch das kartellrechtswidrige Verhalten einen Schaden erlitten haben.

Selbst wenn kein Verstoß festgestellt wird, sind allein die kartellrechtlichen Ermittlungen der Behörden an sich zu bedenken. Sie können mehrere Jahre dauern, zu einer Störung des Tagesgeschäfts führen, sind entsprechend kostenintensiv und können den Unternehmensruf schädigen. Die Wettbewerbsbehörden verfügen über weitreichende Ermittlungsbefugnisse, die u. a. auch die Durchsuchung von Geschäfts- und Privaträumen und die Beschlagnahme relevanter Unterlagen umfassen.

4.3 Kartellrechtliche Compliance im Einzelfall

Neben den stets verbotenen bezweckten Beschränkungen des Wettbewerbs gibt es eine Vielzahl an denkbaren Konstellationen, in denen ein Verstoß gegen das Kartellverbot außerdem in Betracht kommen kann.

In Anbetracht der genannten Ziele und der potenziellen Haftungsrisiken des Kartellrechts gilt es, alle Aspekte einer potenziell relevanten Konstellation im Einzelfall zu würdigen, um kartellrechtliche Compliance sicherzustellen. Die Beurteilung einer Vereinbarung, eines Verhaltens oder der Gründung einer Organisation kann je nach wettbewerblichen Umständen und insbesondere den beteiligten Unternehmen verboten oder erlaubt sein. Im Detail kann auch die jeweils verfolgte Zielsetzung neben anderen Faktoren relevant sein.

Daher kann erst auf Basis eines (hinreichend) konkretisierten Sachverhalts belastbar geprüft werden, ob sich die Beteiligten kartellrechtskonform verhalten. Eine rein abstrakte Prüfung ist nicht möglich. Die nachfolgenden Ausführungen skizzieren mithin nur die Grenzen, innerhalb derer sich das Cyber-Bündnis, die einzelnen Waben und die beteiligten Unternehmen mindestens bewegen müssen. Unabhängig davon ist bei Zweifeln stets eine eigenverantwortliche Prüfung durch das beteiligte Unternehmen erforderlich, um Compliance sicherzustellen.

4.4 Vorliegend besonders relevante Aspekte des Kartellrechts

Im Folgenden werden aus kartellrechtlicher Sicht besonders relevante Aspekte skizziert.

4.4.1 Kartellrechtskonformer Informationsaustausch bei einem Vorfall

Im Rahmen des allgemeinen Kartellverbots ist auch der (evtl. sogar nur einseitige) Austausch wettbewerblich sensibler Informationen zwischen (potenziellen) Wettbewerbern untersagt. Auf dieses Verbot des Informationsaustauschs ist stets besonders zu achten. Für weitere Details sowie Ausführungen allgemein zur Best Practice wird auf den VDMA-Verhaltenskodex (Code of Conduct) von 2017 verwiesen.

Für das Cyber-Bündnis bedeutet das: Ein/e IT-Mitarbeiter/in darf beispielsweise beim Einsatz in einem anderen im Wettbewerb stehenden Unternehmen keine wettbewerblich sensiblen Informationen weitergeben und sollte solche nach Möglichkeit auch nicht von dem Unternehmen entgegennehmen. Auch dürfen keine derartigen Informationen indirekt über einen Dritten sozusagen „über die Bande“ ausgetauscht werden (sogenannte Hub-and-spoke-Konstellation). Selbst wenn der Betrieb des Cyber-Bündnisses also über den VDMA oder eine zu gründende Organisation abliefe, ist der Austausch wettbewerblich sensibler Informationen zwischen den im (potenziellen) Wettbewerb stehenden und sich unterstützenden Unternehmen problematisch.

Eine denkbare Maßnahme, um Risiken zu reduzieren, ist die Organisation in Form der Waben. Zudem könnten zur Risikominimierung Branchengruppen gebildet werden, sodass in einer Wabe keine (potenziellen) Wettbewerber organisiert sind und/oder im Bedarfsfall Unterstützung nur durch Unternehmen geleistet wird, die nicht im (potenziellen) Wettbewerb mit dem Unternehmen stehen, dem Hilfe geleistet wird. Darüber hinaus müssen präventiv Vertraulichkeitsvereinbarungen (NDAs) zwischen den beteiligten Unternehmen, aber auch mit den eingesetzten Mitarbeitenden abgeschlossen werden, um die Weitergabe von wettbewerblich relevanten Informationen (in beide Richtungen) zu unterbinden und damit eine auch nur mögliche Abstimmung des wettbewerblichen Verhaltens der beteiligten Unternehmen zu verhindern. Ohne den Abschluss solcher NDAs besteht ein erheblich gesteigertes Risiko des kartellrechtswidrigen Informationsaustausches zwischen einander unterstützenden (potentiellen) Wettbewerbern.

4.4.2 Regelbetrieb (ohne Vorfall/Krise)

4.4.2.1 Aufnahme neuer Mitglieder (Beitrittsvoraussetzungen)

Auch wenn die Mitgliedsunternehmen keine Marktmacht haben, ist es empfehlenswert, die Aufnahme neuer Bündnismitglieder stets an gleiche Voraussetzungen zu knüpfen. Die Voraussetzungen sollten

ferner nicht zu hoch sein, also grundsätzlich von Unternehmen erfüllt werden, die Vorkehrungen in einem Maß getroffen haben, das von einem Unternehmen der betreffenden Größe in technischer und organisatorischer Hinsicht vernünftigerweise erwartet werden darf. Damit lässt sich potenziell denkbarer Streit vermeiden.

4.4.2.2 Informationsaustausch

Zum Informationsaustausch im Rahmen der allgemeinen Zusammenarbeit (d. h. nicht im Kontext eines Vorfalls/einer Krise) wird auf den VDMA-Verhaltenskodex (Code of Conduct) von 2017 verwiesen, welcher insbesondere Ausführungen zur Best Practice enthält.

4.4.2.3 Rechte und Pflichten für Mitglieder, insbesondere Wettbewerbsverbot

Die Rechte und Pflichten der Bündnismitglieder sollten vorsorglich nicht verbindlich ausgestaltet werden.

So könnte insbesondere die Pflicht, Leistungen im Cyber-Bündnis in Anspruch zu nehmen (und also keinen externen Dienstleister zu beauftragen) oder Leistungen nur im Netzwerk anzubieten (also nicht gegenüber externen Dritten), ein Wettbewerbsverbot darstellen.

Solange die betreffenden Vereinbarungen eine Beschränkung des Wettbewerbs nicht bezwecken, sondern „nur" bewirken, wären sie im Grundsatz kartellrechtlich aber vermutlich zulässig, solange die Mitgliedsunternehmen einen geringen Marktanteil für IT-Dienstleistungen aufweisen. Eine horizontale bzw. vertikale Vereinbarung und deren wettbewerblichen Auswirkungen werden regelmäßig im Rahmen des behördlichen Ermessens als geringfügig („de-minimis")[4] angesehen bzw. keine „spürbare"[5] Beeinträchtigung beigemessen, wenn die beteiligten Unternehmen zusammen bzw. jeweils zumindest weniger als 10 % Marktanteil auf dem relevanten Markt, hier für IT-Dienstleistungen, haben. Das Bundeskartellamt sieht in solchen Fällen von einer Verfahrenseinleitung ab. Andernfalls und über die genannte Schwelle hinaus käme zudem eine Einzelfreistellung in Betracht. Die Schwelle senkt sich auf 5 %, sofern 30 % oder mehr des betroffenen Marktes von der Gesamtheit der angestrebten Waben bzw. dem gesamten Cyber-Bündnis abgedeckt wird.[6] Im Falle von sog. Kernbeschränkungen[7] ist eine Geringfügigkeit (und regelmäßig ebenso eine Einzelfreistellung) jedoch ausgeschlossen.

[4] Vgl. auch für weitere Konkretisierungen: Bekanntmachung Nr. 18/2007 des Bundeskartellamtes über die Nichtverfolgung von Kooperationsabreden mit geringer wettbewerbsbeschränkender Bedeutung („Bagatellbekanntmachung") vom 13. März 2007.

[5] Vgl. auch für weitere Konkretisierungen: Mitteilung der Kommission – Bekanntmachung über Vereinbarungen von geringer Bedeutung, die im Sinne des Artikels 101 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union den Wettbewerb nicht spürbar beschränken (De-minimis-Bekanntmachung).

[6] Sog. kumulativer Abschottungseffekt im Falle von nebeneinander bestehenden Netzen von Vereinbarungen verschiedener Lieferanten oder Händler für den Verkauf von Waren oder das Angebot von Dienstleistungen, die ähnliche Wirkungen auf dem Markt haben.

[7] Dies sind Vereinbarungen, die unmittelbar oder mittelbar, für sich allein oder in Verbindung mit anderen Umständen unter der Kontrolle der Vertragsparteien Folgendes bezwecken oder bewirken: a) im Hinblick auf Dritte die Festsetzung von Preisen oder Preisbestandteilen beim Einkauf/Verkauf von Erzeugnissen bzw. beim Bezug/Erbringung von Dienstleistungen sowie b) die Beschränkung von Produktion, Bezug oder Absatz von Waren oder Dienstleistungen, insbesondere durch die Aufteilung von Versorgungsquellen, Märkten oder Abnehmern.

4.4.3 Wettbewerbsbeschränkung durch Zusammenarbeit (Einkaufsgemeinschaft)

In Bezug auf die angedachte Kooperation bei der gemeinsamen Beschaffung von Equipment o. ä. (s. o.) dürfte eine Bündelung der Nachfrage als Beeinflussung des Wettbewerbs auch in diesem Kontext als eine denkbare Wettbewerbsbeschränkung wahrscheinlich freigestellt sein bzw. diese regelmäßig im Rahmen des behördlichen Ermessens als geringfügig („de-minimis") angesehen bzw. ihr keine „spürbare" Beeinträchtigung beigemessen werden.

Speziell in Bezug auf KMUs sehen darüber hinaus die zuständigen Behörden bei Einkaufskooperationen, die einen gemeinsamen Marktanteil von weniger als 15 % auf den betroffenen Einkaufs- bzw. Verkaufsmärkten halten, einen Kartellverstoß als unwahrscheinlich bzw. jedenfalls eine Einzelfreistellung als wahrscheinlich an.[8]

5. Datenschutz und Cybersecurity

5.1 Datenschutz allgemein

Grundsätzlich gilt, dass auch bzw. erst recht bei einem Vorfall bzw. in einer Krise der Datenschutz einzuhalten ist (kein Dispens des Datenschutzrechts). Zu den wichtigsten Datenschutzgrundsätzen aus Art. 5 DSGVO zählt der Zweckbindungsgrundsatz, nach dem personenbezogene Daten (alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, Art. 4 Nr. 1 DSGVO) nur für bestimmte festgelegte Zwecke (hier: Hilfeleistung bei einem Vorfall/einer Krise) verarbeitet, also u. a. erhoben, gespeichert und genutzt, werden dürfen. Eine zweckwidrige Verarbeitung ist unzulässig.

5.2 Datenschutzrechtliche Verantwortlichkeit; Wahrung der datenschutzrechtlichen Grundsätze

Eine wesentliche Frage betrifft die datenschutzrechtliche Verantwortlichkeit. Datenschutzrechtlich verantwortlich ist grundsätzlich das Unternehmen, das allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 4 Nr. 7 DSGVO).

In der Regel ist also das betroffene und Hilfe suchende Unternehmen datenschutzrechtlich Verantwortlicher. Aus dieser Verantwortlichkeit folgt die umfassende Pflicht zur Wahrung des Datenschutzes und zwar allen (potenziell) Betroffenen gegenüber: etwa den eigenen und fremden Mitarbeitenden, Kundinnen und Kunden sowie Lieferantinnen und Lieferanten. Demnach sind die eigenen Mitarbeitenden auf das Datengeheimnis zu verpflichten (datenschutzrechtliche Pflicht auch unabhängig von

[8] Vgl. auch für weitere Konkretisierungen: Merkblatt des Bundeskartellamtes über Kooperationsmöglichkeiten für kleinere und mittlere Unternehmen, Rn. 38.

einem Vorfall) und auch die übrigen Datenschutz-Standards wie die Pflichtinformationen über die Verarbeitung personenbezogener Daten nach Art. 12 ff. DSGVO müssen vorliegen. Die Szenarien „Vorfall“ und „Hilfeleistung“ sollten in diesen Standards sowie ggf. in einer Datenschutz- und IT-Richtlinie adressiert werden.

Wichtig ist auch das Recht auf Datenlöschung (Art. 17 DSGVO), wonach verarbeitete personenbezogene Daten nach Zweckerreichung (hier: Beendigung der Hilfeleistung bzw. des Vorfalls/der Krise) zu löschen sind, wenn nicht aus anderen Gründen eine fortwährende Pflicht bzw. ein fortwährendes Recht zur Verarbeitung und Aufbewahrung besteht.

Ein wesentliches Element der Verantwortlichkeit ist bei einem Vorfall, der mit großer Wahrscheinlichkeit auch mit einer Verletzung des Schutzes personenbezogener Daten („data breach“) einhergehen kann, die Prüfung der Frage, ob eine Melde- und Informationspflicht nach Art. 33, 34 DSGVO besteht. Bei einem potenziellen Risiko für die Rechte und Freiheiten der betroffenen Personen (etwa bei einem möglichen „Identitätsdiebstahl“) ist die zuständige Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden des „data breaches“ zu informieren (Art. 33 DSGVO). Bei einem potenziellen hohen Risiko für die Rechte und Freiheiten der betroffenen Personen (wenn besonders sensible personenbezogene Daten betroffen sind) sind diese – zusätzlich zur Meldung an die Aufsichtsbehörde – unverzüglich zu informieren (Art. 34 DSGVO).

Die Prüfung der Melde- und Informationspflicht muss in jedem Einzelfall und besonders sorgfältig erfolgen. Denn bei einem „data breach“ drohen aufsichtsbehördliche Bußgelder und zivilrechtliche Schadensersatzansprüche, die ggf. höher ausfallen können, wenn eine Melde- oder Informationspflicht nicht erfüllt wurde.

5.3 Auftragsverarbeitung und gemeinsame Verantwortlichkeit

Das Hilfe leistende Unternehmen dürfte regelmäßig als Auftragsverarbeiter (Art. 28 DSGVO) zu qualifizieren sein, also weisungsgebunden entsprechend einem externen IT-Dienstleister, für das betroffene Unternehmen (als datenschutzrechtlich Verantwortlichem) tätig werden. Hierfür bedarf es einer entsprechenden datenschutzrechtlichen Vereinbarung, die vorsorglich wechselseitig zwischen den Bündnismitgliedern geschlossen werden sollte (siehe **Muster Vereinbarung über die datenschutzrechtliche Auftragsverarbeitung** auf der Website).

Gegebenenfalls und insbesondere abhängig von der Organisationsform des jeweiligen Cyber-Bündnisses (hierzu siehe unter Teil „Organisation“) kommt auch eine sog. gemeinsame Verantwortlichkeit (Art. 26 DSGVO) in Betracht, etwa im Hinblick auf ein gemeinsam betriebenes Schulungs-, Informati-

ons-, oder Datensicherungsportal. Kennzeichnend hierfür ist, dass mehrere Verantwortliche gemeinsam und gleichberechtigt über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Auch dies ist im Einzelfall zu prüfen und es bedarf einer entsprechenden datenschutzrechtlichen Vereinbarung (siehe **Muster Verarbeitung über die gemeinsame datenschutzrechtliche Verantwortlichkeit** auf der Website).

Je nach Organisationsform und organisatorischer Verfestigung und Komplexität des Cyber-Bündnisses kann es sich anbieten, die genannten Vereinbarungen nach Art. 26 und Art. 28 DSGVO auch in ein übergreifendes und sämtliche Konstellationen adressierendes sogenanntes Intragroup Agreement zu überführen, um zahlreiche bilaterale Vereinbarungen zu vermeiden und eine bessere Administration und Übersichtlichkeit zu erreichen.

5.4 Arbeitnehmerdatenschutz

Bezüglich des Arbeitnehmerdatenschutzes wird auf die obigen Ausführungen zum Arbeitsrecht unter Ziff. 3.2 verwiesen.

5.5 IT-Sicherheit („TOMs"; Informationssicherheitsmanagementsystem (ISMS))

Empfehlenswerte Standards und Best Practices bezüglich der Implementierung und Aufrechterhaltung angemessener, risikoadäquater IT-Sicherheit bzw. eines Informationssicherheitsmanagementsystems (ISMS) sind die ISO-Normen (insbes. 27001) und der Grundschutzkatalog sowie die Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI)[9]. Zu den technischorganisatorischen Schutzmaßnahmen („TOMs" nach Art. 32 DSGVO) s. o. zu IT Compliance und Risk unter Ziff. 1.4.2).

Festzuhalten ist, dass es (auch) bezüglich IT-Sicherheit und der einzusetzenden technischen und organisatorischen Schutzmaßnahmen (siehe Art. 32 DSGVO) keine „one size fits all"-Lösung gibt. Vielmehr ist das angemessene Maß an IT-Sicherheit von der Cyber-Risk-Exposure (s. o. Ziff. 1.3.1) im Einzelfall abhängig.

6. Steuerrechtliche Aspekte

Im Hinblick auf die steuerrechtlichen Aspekte eines Cyber-Bündnisses ist zwischen den einzelnen unter A.2. beschriebenen Modellen zu unterscheiden sowie nach ertragsteuerlichen und umsatzsteuerlichen Aspekten.

[9] Kostenfrei abrufbar mit zahlreichen weiteren Informationen unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

6.1 Modell 1: „Handschlag“-Vereinbarung

6.1.1 Umsatzsteuerliche Aspekte

Aus umsatzsteuerlicher Sicht würde sich vorliegend die Frage stellen, ob und inwieweit die einzelnen Hilfsmaßnahmen der Bündnismitglieder gegebenenfalls umsatzsteuerbar und umsatzsteuerpflichtig sind. Wir gehen davon aus, dass die einzelnen Beiträge der Bündnismitglieder unentgeltlich erbracht werden.

Im Rahmen des Modells 1 liegt rechtlich entweder eine Innengesellschaft im Sinne von §§ 705 ff. BGB vor oder es liegt aufgrund fehlenden Rechtsbindungswillens keine solche Gesellschaft vor und die einzelnen Bündnismitglieder erbringen die Leistungen im jeweils bilateralen Verhältnis.

Soweit es sich um eine Innengesellschaft handelt, sollten die einzelnen Maßnahmen der Bündnismitglieder Gesellschafterbeiträge darstellen, die gegebenenfalls als eine umsatzsteuerpflichtige unentgeltliche Wertabgabe im Sinne von § 3 Abs. 9a UStG qualifizieren. Denn den einzelnen Maßnahmen sollten Kosten zugrunde liegen, z. B. Personalkosten und dem einzelnen Bündnismitglied wird jeweils ein individueller und unmittelbarer wirtschaftlicher Vorteil zugewendet.

Voraussetzung dafür wäre aber weiter, dass die unentgeltliche Dienstleistung zu außerunternehmerischen Zwecken erfolgt. Dagegen sprechen vorliegend gute Argumente, da die Beistandshilfe im Gegenseitigkeitsverhältnis steht und somit ein unternehmerisches Interesse an der aktiven Teilnahme an einem solchen Cyber-Bündnis besteht. Die IT-Sicherheit ist ein unternehmerischer Belang, welchen es schon aus rechtlichen Gründen zu optimieren gilt. Insoweit sollte die Beteiligung an einem Cyber-Bündnis auch grundsätzlich eine geeignete Maßnahme darstellen, um die IT-Sicherheit im eigenen Unternehmen zu erhöhen.

Für diese Auslegung spricht auch die veröffentlichte Auffassung der Finanzverwaltung, die bei kostenloser Unterstützung bei Arbeitsgemeinschaften oder Konsortien grundsätzlich von einer nicht umsatzsteuerbaren Leistung ausgeht, zumindest soweit die erbrachten Beiträge den Vereinbarungen entsprechen (A 1.6 UStAE Abs. 8). Gleichwohl verbleibt eine gewisse Restunsicherheit, die aufgrund des jeweiligen Transaktionsvolumens vorab mittels einer verbindlichen Auskunft abgesichert werden sollte.

Ein höheres Risiko einer umsatzsteuerpflichtigen unentgeltlichen Wertabgabe dürfte bei einer losen Vereinbarung ohne Rechtsbindungswillen bestehen, unter anderem, weil diese nicht zwingend im Gegenseitigkeitsverhältnis steht und der unternehmerische Zweck daher fraglich sein könnte.

Soweit es sich um umsatzsteuerpflichtige Wertabgaben handelt, würden diese sich im Falle von unentgeltlichen Dienstleistungen gemäß § 10 Abs. 4 Nr. 3 UStG nach den bei der Ausführung des Umsatzes entstandenen Ausgaben bemessen. Erfasst werden demnach sämtliche Ausgaben, also auch anteilige Personal- oder Versicherungskosten. Würden z. B. fünf (5) Mitarbeitende einen Tag lang Leistungen im Rahmen des Cyber-Bündnisses erbringen, dürften die entsprechenden Bruttolohnkosten die Mindestbemessungsgrundlage für die umsatzsteuerpflichtige Wertabgabe bilden.

6.1.2 Ertragsteuerliche Aspekte

In ertragsteuerlicher Hinsicht würde sich vorliegend beim Modell 1 insbesondere die Frage stellen, inwieweit Aufwendungen der Bündnismitglieder, die auf die Hilfsmaßnahmen entfallen, noch als Betriebsausgaben abzugsfähig sind. Bei der Innengesellschaft dürfte es sich ertragsteuerlich um ein transparentes Vehikel handeln, sodass die Maßnahmen den jeweiligen Mitgliedern unmittelbar zugerechnet werden.

Nach § 4 Abs. 4 EStG sind Betriebsausgaben Aufwendungen, die durch den Betrieb veranlasst sind. Daran könnte vorliegend gezweifelt werden, weil die Aufwendungen für Hilfsmaßnahmen nicht dem eigenen Unternehmen, sondern einem fremden Dritten zugutekommen.

Betrieblich veranlasst sind alle Aufwendungen, die objektiv, d. h. tatsächlich oder wirtschaftlich, in einem Zusammenhang mit dem Betrieb stehen und subjektiv dem Betrieb zu dienen bestimmt sind. Abzustellen sind auf die Gründe, die den Steuerpflichtigen bewogen haben, die Kosten zu tragen. In der vorliegenden Konstellation dient das Cyber-Bündnis der IT-Sicherheit der einzelnen Mitglieder. Die Maßnahmen sollten zumindest bei der Innengesellschaft in einem rechtlichen Gegenseitigkeitsverhältnis stehen. Daher ließe sich wohl grundsätzlich auch argumentieren, dass Hilfsmaßnahmen im Beistandsfall auch dem eigenen Betrieb dienen. Gleichwohl ist bei diesem Modell nicht ohne Weiteres klar, worin genau die gegenseitigen Beiträge bestehen und inwieweit sie rechtlich durchsetzbar sind. Daher ist es möglich, dass im Rahmen einer Betriebsprüfung dieses Thema seitens der Finanzverwaltung aufgegriffen werden könnte.

6.2 Modell 2: „Handschlag plus Standard- und Musterverträge“

6.2.1 Umsatzsteuerliche Aspekte

Beim Modell 2 dürfte es sich rechtlich um eine Innengesellschaft handeln – abhängig von der konkreten Ausgestaltung der Verträge. Daher gelten die vorstehenden Ausführungen zur Innengesellschaft unter 6.1.1. grundsätzlich entsprechend. Zusätzliches Argumentationspotenzial für die nicht vor-

liegende Umsatzsteuerbarkeit sollte bei diesem Modell durch die Festlegung der einzelnen Beiträge in den Verträgen erzielt werden. So dürfte sich noch besser argumentieren lassen, dass die Beiträge insoweit im unternehmerischen Interesse stehen und ein direkter Zusammenhang zur Unternehmenstätigkeit besteht. Gleichwohl wäre auch hier die Absicherung des Risikos der Umsatzsteuerpflicht mittels einer verbindlichen Auskunft ratsam.

6.2.2 Ertragsteuerliche Aspekte

Beim Modell 2 stellen sich ebenso Fragen nach der Abzugsfähigkeit der Aufwendungen für das Cyber-Bündnis als Betriebsausgaben. Auch hier sollte mangels Gewinnerzielungsabsicht grundsätzlich eine ertragsteuerliche transparente Innengesellschaft vorliegen.

Die Kosten für die einzelnen Maßnahmen müssten also vorliegend auch betrieblich veranlasst sein. Im Gegensatz zu dem Modell 1 sollten bei diesem Modell die Beiträge der Mitglieder zu dem Cyber-Bündnis aber eindeutig und rechtlich bindend geregelt sein. Daher dürfte das Argumentationspotenzial für eine betriebliche Veranlassung bei diesem Modell wesentlich stärker ausgeprägt sein, da Unterstützungsmaßnahmen eines Bündnismitglieds wahrscheinlich nur erfolgen, wenn diese im Gegenseitigkeitsverhältnis stehen. Soweit kein Gegenseitigkeitsverhältnis vorliegt und dennoch Maßnahmen erfolgen, könnte nach dem betrieblichen Nutzen und der Motivation gefragt werden. Soweit hier keine plausible Erklärung des relevanten Bündnismitglieds erfolgen kann, dürfte der Betriebsausgabenabzug fraglich sein.

6.3 Modell 3: Organisation in verbindlicher Form (etwa als GmbH)

6.3.1 Umsatzsteuerliche Aspekte

Bei einer verfestigten Organisationsstruktur wie z. B. bei einem eingetragenen Verein oder einer GmbH besteht ebenfalls das Risiko einer umsatzsteuerpflichtigen Leistungserbringung, wenn Hilfsmaßnahmen durchgeführt werden.

Es ist allgemein anerkannt, dass ein Verein oder eine GmbH grundsätzlich umsatzsteuerpflichtige Leistungen an ihre Gesellschafter bzw. Mitglieder erbringen kann. Soweit dem kein Entgelt gegenübersteht, etwa in Form von Mitgliedsbeiträgen oder Gebühren, sollten unentgeltliche Wertabgaben nach § 3 Abs. 1b UStG und § 3 Abs. 9a UStG in Betracht kommen. Für die weitere umsatzsteuerliche Beurteilung kommt es auf die genaue Struktur und Rechtsform an. Unentgeltliche Leistungen, die eine GmbH an ihre Gesellschafter erbringt, dürften grundsätzlich umsatzsteuerpflichtige Wertabgaben darstellen. Sollte das Modell 3 daher näher in Betracht kommen, sollten die umsatzsteuerlichen Aspekte spezifischer geprüft und bei der Wahl des Modells berücksichtigt werden.

6.3.2 Ertragsteuerliche Aspekte

Auch im Hinblick auf die ertragsteuerlichen Aspekte dürften – abhängig von der Rechtsform – eher nachteilige Konsequenzen, wie z. B. verdeckte Gewinnausschüttungen und Nichtabziehbarkeit von für die Hilfsmaßnahmen aufgewendete Betriebsausgaben in Betracht kommen. Dies könnte z. B. der Fall sein, wenn eine GmbH unentgeltliche Dienstleistungen an ihre Gesellschafter erbringt.

Anhang 2: Musterverträge und -texte

Diese Vertragsmuster wurden mit großer Sorgfalt erstellt und gemäß der Idee und den Maßgaben dieses Leitfadens aufgesetzt. Sie erheben aber als Muster keinen Anspruch auf Vollständigkeit und Richtigkeit für den jeweiligen Einzelfall und ersetzen keine Rechtsberatung.

Die Vertragsmuster sind vielmehr ein allgemeiner Vorschlag für eine mögliche Regelung. Vor einer unveränderten Übernahme des gesamten jeweiligen Inhaltes muss daher im eigenen Interesse sorgfältig und eigenverantwortlich überprüft werden, ob und in welchen Teilen gegebenenfalls eine Anpassung an die konkret zu regelnde Situation und die Rechtsentwicklung erforderlich ist. Auf diesen Vorgang hat die Allianz Industrie 4.0 Baden-Württemberg keinen Einfluss und kann daher für die Nutzung und Auswirkungen dieser Vertragsmuster keine Haftung übernehmen. Falls Sie eine den konkreten Parteien und Umständen direkt angepasste Vereinbarung benötigen, sollten Sie sich durch einen sachkundigen Rechtsanwalt beraten lassen.

- Arbeitsvertragsklauseln zum Einsatz bei kritischen Vorfällen
- Betriebsvereinbarung zur Lage und Dauer der Arbeitszeit bei kritischen Vorfällen
- Betriebsvereinbarung zur Vorgehensweise bei kritischen Vorfällen
- Betriebsvereinbarung zur Datennutzung bei kritischen Vorfällen
- Geheimhaltungserklärung (NDA) Mitarbeiter
- Geheimhaltungsvereinbarung (NDA) Unternehmen
- Verpflichtung auf das Datengeheimnis
- Vereinbarung über die datenschutzrechtliche Auftragsverarbeitung
- Vereinbarung über die gemeinsame datenschutzrechtliche Verantwortlichkeit

Die Musterverträge stehen online auf der Website der Allianz Industrie 4.0 Baden-Württemberg zum Abruf und Download zur Verfügung.

Allianz Industrie 4.0 Baden-Württemberg
VDMA e. V. Baden-Württemberg
Kronenstraße 3
70173 Stuttgart

Tel.: +49 711 22801-20
E-Mail: info@i40-bw.de
Internet: www.i40-bw.de

Gefördert durch:

Baden-Württemberg
MINISTERIUM FÜR WIRTSCHAFT, ARBEIT UND TOURISMUS

Mit Unterstützung von:

VDMA