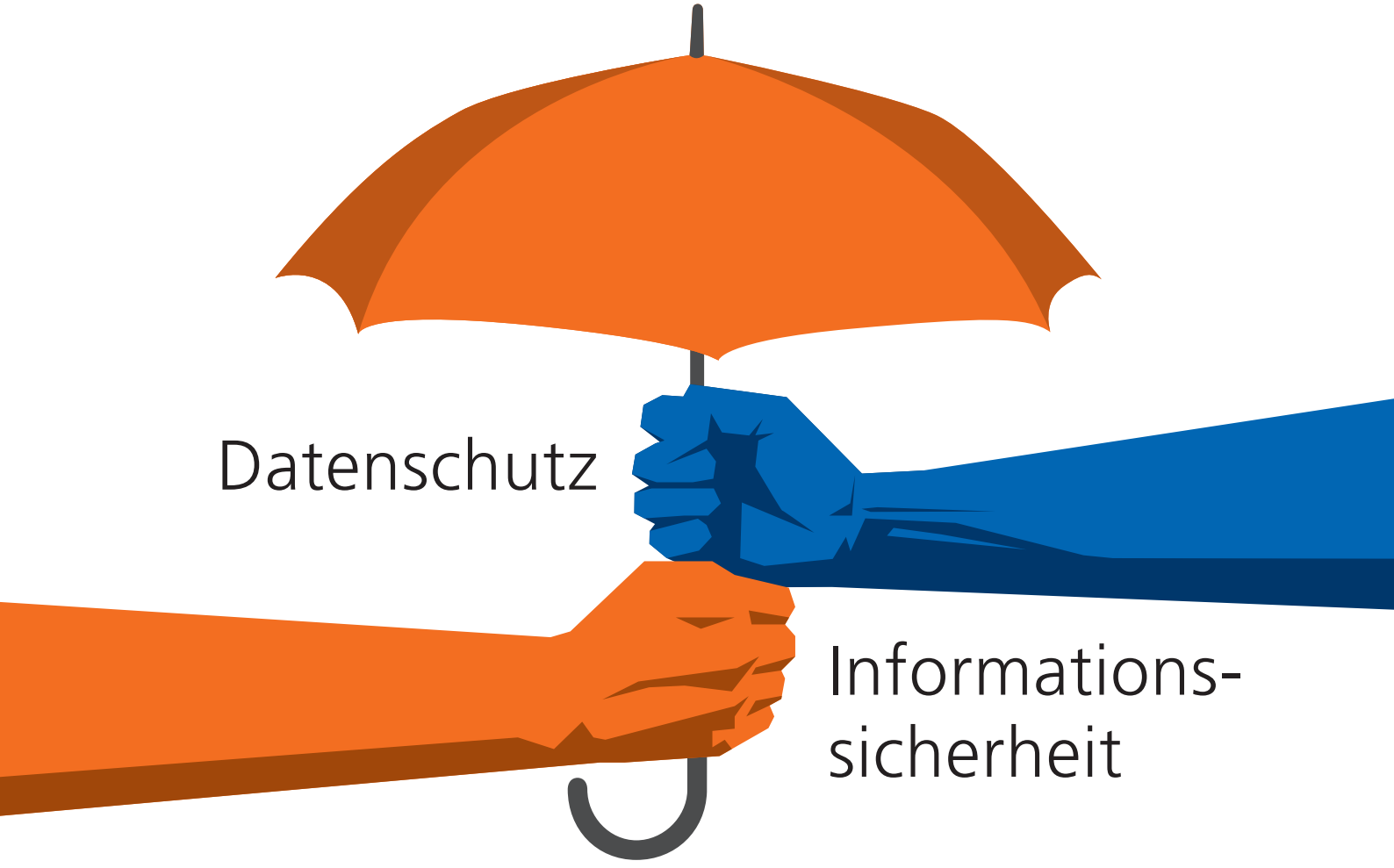
DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner

AUSGABE 2/2022



IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 28, 2/2022
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Norbert Schäfer

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 580024-0, Telefax 069 580024-900, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Mona Baitinger, Jenny Engemann, Claudia Gerst, Derya Isikli, Jens Saenger, Jörg Scharditzky, Lars Schinnerling, Katja Schlüter, Maximilian Schmidt, Thomas Schröder, Benjamin Wellnitz

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto (Titel)
Gestaltung: Ralf Egenolf
Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktionsschluss: 9. September 2022
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc

Jens Saenger
Sprecher der Geschäftsführung

Schon vor der Pandemie stand die Kreditwirtschaft zahlreichen Herausforderungen gegenüber. Neben der Null-Zins-Politik beschäftigten vor allem der Digitalisierungsdruck und der sich verändernde Markt die Finanzbranche. Mit Corona wurden dann weltweite Lieferketten unterbrochen, die Wirtschaft brach ein. Es ist bemerkenswert, wie stressresistent sich die Institute im Großen und Ganzen gaben. Man hätte sich mehr Zeit gewünscht, um die positiven Impulse, beispielsweise auf die Digitalisierung, zu konsolidieren und umzusetzen.

Aber das Zeitfenster ist denkbar eng. Nahezu übergangslos wurde mit dem russischen Angriff auf die Ukraine die europäische Sicherheitskultur in Frage gestellt. Damit verbunden sehen wir uns mit einer noch nicht dagewesenen Energiekrise konfrontiert. Um der damit einhergehenden Inflationsentwicklung zu begegnen, hat die EZB den Leitzins (deutlich) erhöht. Doch auch das birgt – nicht nur für die Bankenbranche – (Rezessions-)Risiken. Als wäre das alles nicht genug, sind stärker als zuvor die Herausforderungen eines immer enger werdenden Arbeitsmarktes zu managen.

In diesem Sinne ist es unser Anliegen, Sie in diesen Zeiten durch unsere Dienstleistungen – wo immer möglich – zu unterstützen.

Herzlichst

Ihr Jens Saenger

▶ **Datenschutz**

Drittlandsübertragung von personenbezogenen Daten

Eine Übermittlung von personenbezogenen Daten an sogenannte Drittländer – Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums – kommt häufig bei der Nutzung von Social-Media-Angeboten oder Microsoft-Diensten vor. Doch was ist bei der Drittlandsübertragung zu beachten und wie genau ist dies aus Datenschutzsicht zu prüfen?

Bei der Übertragung von personenbezogenen Daten in Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums (= Drittländer)[1] gelten gesonderte Anforderungen der Europäische Datenschutz-Grundverordnung (DSGVO). Dabei kann entweder eine Auftragsdatenverarbeitung gem. Art. 28 DSGVO vorliegen oder aber eine gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO.

Angemessenheitsbeschluss

Grundsätzlich ist eine Übermittlung von personenbezogenen Daten in ein Drittland, also außerhalb des Europäischen Wirtschaftsraums, nur dann rechtmäßig und DSGVO-konform, wenn gem. Art. 44 Satz 1 i. V. m. Art. 45 Abs. 1 Satz 1 DSGVO ein angemessenes Schutzniveau besteht.

Art. 45 Abs. 1 Satz 1 DSGVO bestimmt, dass ein angemessenes Schutzniveau in einem Drittland gegeben ist, soweit für dieses Drittland ein entsprechender Beschluss im Sinne von Art. 288 Abs. 4 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) gem. Art. 45 Abs. 3 DSGVO gegeben ist. Dies bedeutet in der Praxis, dass die jeweilige Übermittlung im konkreten Einzelfall die Voraussetzungen sowie vorhandene Anforderungen des jeweiligen Beschlusses erfüllen muss.

Ein Transfer von Daten auf Grundlage eines Angemessenheitsbeschlusses genießt das Sonderrecht, dass die Übermittlung der Daten in ein Drittland einem Transfer innerhalb der EU gleichgestellt wird.

Derzeit gibt es für 14 Staaten einen Angemessenheitsbeschluss. Diese sind: Andorra, Argentinien, Färöer-Inseln, Guernsey, Isle of Man, Israel, Japan, Jersey, Kanada, Neuseeland, Republik Korea (Südkorea), Schweiz, Uruguay, Vereinigtes Königreich. Die Liste kann auf der Webseite der Europäischen Kommission eingesehen werden unter https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_6916.

Garantien und Ausnahmen

Sofern kein angemessenes Schutzniveau durch einen Angemessenheitsbeschluss gem. Art. 45 Abs. 3 DSGVO gegeben sein sollte, kann eine Drittlandsübertragung beispielsweise über geeignete Garantien oder Ausnahmen rechtmäßig erfolgen.

Diese geeigneten Garantien werden in Art. 46 ff. DSGVO geregelt. Diese können zum Beispiel aus

- „Binding Corporate Rules“ (BCRs) gem. Art. 46 Abs. 2 lit. b DSGVO, bei denen es sich um verbindliche interne Datenschutzvorschriften handelt,
- „EU Model Clauses“ (Standartvertragsklauseln, kurz SCC – abgekürzt von englisch Standard Contractual Clauses) gem. Art. 46 Abs. 2 lit. c bzw. d DSGVO (auf die im Folgenden kurz eingegangen werden soll),
- „Code of Conduct“ (Verhaltensregeln) gem. Art. 46 Abs. 2 lit. e DSGVO,
- Zertifizierung gem. Art. 46 Abs. 2 lit. f DSGVO i. V. m. Art. 42 DSGVO und
- behördlich genehmigten Vertragsklauseln gem. Art. 46 Abs. 3 lit. a DSGVO bestehen.

Ebenso enthält Art. 49 DSGVO Ausnahmen, wenn weder ein Beschluss nach Art. 46 Abs. 1 DSGVO noch Garantien gem. Art. 46 Abs. 2 ff DSGVO gegeben sind. Danach ist eine Übermittlung rechtmäßig und entspricht dem Grundsatz eines angemessenen Schutzniveaus auch dann, wenn die Voraussetzungen des Art. 49 DSGVO erfüllt sind.

Ausnahmen nach Art. 49 DSGVO können sein:

- die Einholung einer qualifizierten Einwilligung der betroffenen Person gem. Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO oder
- vertragliche und vorvertragliche Übermittlungen zwischen der betroffenen Person und dem Verantwortlichen gem. Art. 49 Abs. 1 UAbs. 1 lit. b bzw. c DSGVO,
- die Übermittlung aus wichtigen Gründen des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d DSGVO),
- die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e DSGVO),
- die Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen (Art. 49 Abs. 1 UAbs. 1 lit. f DSGVO) oder
- die Übermittlung aus einem Register, das gemäß dem Recht der Union oder der Mitgliedsstaaten zur Information der Öffentlichkeit bestimmt ist (Art. 49 Abs. 1 UAbs. 1 lit. g DSGVO).

Art. 46 Abs. 2 DSGVO gibt eine gewisse Reihenfolge zur Umsetzung einer DSGVO-konformen Drittlandsübertragung von personenbezogenen Daten vor:

Wenn ein angemessenes Schutzniveau gem. Art. 45 Abs. 3 DSGVO vollumfänglich vorliegen sollte, werden keine weiteren geeigneten Garantien gem. Art. 46 f. DSGVO oder die Berücksichtigung von Ausnahmeregelungen nach Art. 49 DSGVO benötigt.

Sofern weder ein angemessenes Schutzniveau gem. Art. 45 Abs. 3 DSGVO noch geeignete Garantien nach Art. 46 f. DSGVO oder Ausnahmeregelungen gem. Art. 49 DSGVO vorliegen, ist von einer nicht materiell rechtmäßigen Drittlandsübertragung auszugehen.

Standardvertragsklauseln

Sofern eine personenbezogene Datenübertragung an ein Drittland erfolgt, handelt es sich häufig um eine Datenübertragung in die USA. Aufgrund des Schrems-II-Urteils vom 16. Juli 2020 des Europäischen Gerichtshofs (EuGH) wurde das Privacy-Shield-Abkommen zwischen der EU und den USA für unwirksam erklärt[2]. In der Praxis werden – bei nicht vorliegendem angemessenen Schutzniveau – häufig die sogenannten Standardvertragsklauseln eingesetzt. >

AUTOREN UND ANSPRECHPARTNER

Derya Isikli
Beauftragte Informationssicherheit & Datenschutz
E-Mail: derya.isikli@dz-cp.de

Benjamin Wellnitz
Bereichsleiter Informationssicherheit & Datenschutz
E-Mail: benjamin.wellnitz@dz-cp.de

Die Europäische Kommission hat im Juni 2021 die neuen Standardvertragsklauseln verabschiedet[3]. Danach müssen die bestehenden Verträge die neuen Anforderungen erfüllen. **Die Übergangsfrist von Bestandsverträgen läuft zum 27. Dezember 2022 ab.** Neuverträge müssen bereits die neuen Anforderungen erfüllen und dürfen sich auf die alten Standardvertragsklauseln nicht beziehen.
Die neuen Standardvertragsklauseln bestehen aus folgenden zentralen Bausteinen/Modulen:

- Modul 1: Datenübermittlung zwischen zwei Verantwortlichen,
- Modul 2: Datenübermittlung Verantwortlicher an Auftragsverarbeiter,
- Modul 3: Datenübermittlung von einem Auftragsverarbeiter an einen (Unter-)Auftragsverarbeiter,
- Modul 4: Datenübermittlung (Rückübermittlung) Auftragsverarbeiter innerhalb der EU an einen Verantwortlichen im Drittland.

Hinsichtlich der USA ist seit dem Schrems-II-Urteil zu beachten, dass die Standardvertragsklauseln bei Datenübermittlungen in Drittstaaten weiterhin angewendet werden können. Das gilt jedoch unter der besonderen Prämisse, dass der Verantwortliche zuvor prüft, ob die Garantien in den Standardvertragsklauseln auch tatsächlich durchgeführt werden können und die Rechte der Betroffenen hierdurch das gleiche Schutzniveau wie in der EU genießen. Dies verdeutlicht, dass die Anwendung der neuen Standardvertragsklauseln mit zusätzlichem Aufwand verbunden ist: Alle Verträge sind zu prüfen und auch der jeweilige Umfang der Regelungen ist zu prüfen. Sofern vertragsrechtlich die Standardvertragsklauseln zum Einsatz kommen, empfehlen wir Ihnen, Ihren Datenschutzbeauftragten zu konsultieren: Ihr Vertragsbestand sollte daraufhin überprüft werden, ob zum einen Verarbeitungen in einem Drittland vorliegen und diese schon die neuen Standardvertragsklauseln anwenden. ▬

Quellen/weiterführende Links zu den Standardvertragsklauseln:

https://lfd.niedersachsen.de/startseite/themen/internationaler_datenverkehr/standardvertragsklauseln/

https://www.2b-advice.com/de/blog/standardvertragsklauseln/

https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/neue-standardvertragsklauseln-2021-das-gibt-es-nun-zu-tun/

[1] Vgl. Zerdick, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 44 Rn. 10
[2] Vgl. Ziegenhorn, Materielle Rechtmäßigkeit von Datenverarbeitung II, Hagen 2022, S. 65
[3] Durchführungsbeschluss (EU) 2021/914 der EU-Kommission v. 04.06.2021 – Az. C (2021) 3972, ABl. EU Nr. L 199/31 vom 07.06.2021

Datenschutz

Umgang mit Datenschutzverletzungen

Die in Artikel 33 und Artikel 34 DSGVO enthaltenen Melde- bzw. Benachrichtigungspflichten sind Teil eines umfassenden Konzeptes aktiver und passiver Transparenzpflichten. Die Praxisrelevanz dieser Bestimmungen wird anhand der von den Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlichten Statistiken eindrücklich belegt. Der folgende Beitrag widmet sich praxisrelevanten Fragen und gibt Lösungsvorschläge im Zusammenhang mit der Behandlung von Datenschutzverletzungen.

Die Berliner Beauftragte für den Datenschutz weist in ihrem Tätigkeitsbericht für 2021 insgesamt 1163 gemeldete Datenschutzverletzungen aus, 238 Meldungen mehr als ein Jahr zuvor. Der Hessische Beauftragte für Datenschutz gibt in seinem Tätigkeitsbericht für 2021 über 2016 Meldungen an, gegenüber 1433 Meldungen im Vorjahr. In Baden-Württemberg wurde ein Rekordwert von 3136 gemeldeten Vorfällen erreicht, 815 Fälle mehr als im Jahr 2020. Verantwortliche in Niedersachsen meldeten im vergangenen Jahr 1673 Datenschutzverletzungen. 2020 waren es noch 989, 2019 insgesamt 824.

Die denkbaren Sicherheitsverletzungen bzw. deren Entstehen können dabei vielfältige Ursachen haben. Dritte können von außen auf die IT-Strukturen einwirken und grundsätzlich gesicherte IT-Systeme kompromittieren, Daten können offen einsehbar auf einem ungesicherten IT-System liegen und durch Fehlverhaltensweisen einzelner Beschäftigter (vorsätzlich oder fahrlässig) veröffentlicht werden.

Zur Abwendung bzw. Begrenzung von reputativen und finanziellen Risiken ist es in jedem Fall notwendig, dass Verfahrensweisen zur Erkennung und Behandlung von Sicherheitsverletzungen in Form eines Data-Breach-Managements vorhanden sind.

Wann und was ist zu melden?

Die Meldepflicht aus Art. 33 DSGVO wird grundsätzlich bei jeder Verletzung der Sicherheit ausgelöst, sofern diese zu einer Vernichtung, Veränderung, einer unbefugten Offenlegung von personenbezogenen Daten oder zum unbefugten Zugang zu solchen Daten führt (im Folgenden auch als Datenschutzverletzung bezeichnet). Im Zusammenhang mit Ransomware-Angriffen stellt sich jedoch bereits hier häufig die Frage, ob eine absolute Gewissheit einer unbefugten Kenntnisnahme verlangt werden kann oder ob bereits die reine Möglichkeit der Kenntnisnahme ausreicht. Nachdem beispielsweise im Frühjahr 2021 bekannt wurde, dass eine Sicherheitslücke bei lokal betriebenen Exchange- Servern durch Hackergruppen massenhaft ausgenutzt wurde, vertraten jedenfalls einige Aufsichtsbehörden die Ansicht, dass eine Meldung bereits im Falle eines nicht rechtzeitig durchgeführten Updates abzugeben ist. Ein offenkundiger „Erfolg“, z. B. in Form einer Verschlüsselung der Daten, war also nicht gefordert.

Eine Ausnahme von der Meldepflicht besteht nach dem Gesetz nur dann, wenn die Sicherheitsverletzung voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Diese Regelung ist Ausprägung des risikobasierten Ansatzes der DSGVO, wonach Verantwortliche einige Pflichten nur dann treffen, wenn z. B. ein Risiko oder ein hohes Risiko vorliegt. Abweichend von diesen gesetzlichen Rechtsbegriffen wird >

von den Aufsichtsbehörden mitunter auch eine Meldepflicht bei „geringen Risiken“ verneint.

Voraussetzung hierfür ist aber ebenfalls eine gewisse Wahrscheinlichkeit, die im Rahmen einer Risikoanalyse – neben der Eintrittsschwere – unter Berücksichtigung bekannter Umstände ermittelt werden muss. Die konkreten Grenzen zwischen Möglichkeit und Wahrscheinlichkeit sind dabei oftmals nur schwer zu ziehen. Um den praktischen Nachweis, wann etwas als wahrscheinlich gilt, zu erbringen, hat es sich in der Praxis als hilfreich erwiesen, vorab gewisse Regelbeispiele zu definieren.

Zudem bedarf es einer methodisch nachvollziehbaren Risikoanalyse, die neben den drohenden physischen, materiellen oder immateriellen Schäden auch die Art der Datenschutzverletzung aufgreifen muss: Insoweit hat die Risikoanalyse also auch die Anzahl der Betroffenen, den Umfang der Daten, die Datenkategorien, die Identifizierbarkeit und die Wahrscheinlichkeit des unbefugten Zugriffs Dritter einzubeziehen.

Nach Art. 34 DSGVO sind darüber hinaus die Betroffenen immer dann zu benachrichtigen, wenn die Sicherheitsverletzung voraussichtlich zu einem hohen Risiko für die Betroffenen führt.

Der Mindestinhalt einer Meldung an die zuständige Behörde ergib sich aus Art. 33 Abs. 3 DSGVO. Die Aufsichtsbehörden bieten jedoch mittlerweile vielfach Vordrucke oder Online-Formulare an, deren Inhalte z. T. weit über die gesetzlich geforderten Angaben hinausgehen. Im Hinblick auf eine eventuell bestehende Schutzwirkung gem. §§ 42 Abs. 4, 43 Abs. 4 BDSG stellt die Nutzung dieser Online-Formulare daher nicht immer die beste Strategie dar.

Einhaltung der Meldefrist

Die Datenschutzverletzung ist durch den Verantwortlichen einer Datenverarbeitung „unverzüglich und möglichst binnen 72 Stunden“ zu melden. Bei der Beurteilung der Frage, ob eine Meldung „unverzüglich“ geschehen ist, sollen die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen (die zum Zeitpunkt der Meldung bereits eingetreten sind) und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Zusätzlich zu dem Kriterium der „unverzüglichen“ Meldung wird als Leitvorgabe ein 72-Stunden-Zeitraum festgelegt, der grundsätzlich nicht überschritten werden soll. Eine kurze Prüfung des Sachverhalts und die Risikoprognose lassen sich meist sehr zügig durchführen, daher sind bestehende Unsicherheiten in Bezug auf die Frist meist irrelevant. Eine unvollständige Ermittlung des Sachstandes (zumindest in Detailfragen) ist als Begründung für eine Überschreitung der Meldepflicht nicht geeignet, da die Möglichkeit einer stufenweisen Meldung besteht.

Wenn dies aufgrund der Umstände erforderlich ist, z. B. bei komplexen und unübersichtlichen Vorfällen, kann eine Meldung im Einzelfall aber auch später als 72 Stunden erfolgen, dies ist jedoch stichhaltig zu begründen. Zudem sind die fehlenden Angaben unverzüglich nachzureichen, sobald diese vorliegen.

Meldepflichten von Auftragsverarbeitern

Da der Auftraggeber im Rahmen der Auftragsverarbeitung voll verantwortlich bleibt und dem Auftragsverarbeiter nur die technisch-infrastrukturelle Umsetzung des Verarbeitungsvorgangs obliegt, ist der Auftraggeber im Falle von Sicherheitsverletzungen auf zeitnahe und umfassende Informationen des Auftragsverarbeiters angewiesen. Das Gesetz sieht daher eine Meldepflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen vor.

Diese Verpflichtung sieht keine risikoorientierte Ausnahme vor. Die Beurteilung, ob eine Datenschutzverletzung vorliegt, obliegt ausschließlich dem Auftraggeber. Folglich hat der Auftragsverarbeiter Sicherheitsverletzungen nicht erst dann zu melden, wenn er den Vorfall bereits ausermittelt hat und für ihn feststeht, dass es sich mit Gewissheit um eine Datenschutzverletzung handelt, sondern er hat auch unverzüglich jeden Verdachtsfall einer Sicherheitsverletzung zu melden.

In diesem Kontext stellt sich die Frage, ob sich der Auftraggeber bei der Berechnung der Meldefrist die Kenntnis des Auftragsverarbeiters über eine Sicherheitsverletzung zurechnen lassen muss, oder ob die gesetzliche Meldefrist erst mit Kenntnisnahme des Auftraggebers beginnt. Hierzu bestehen unterschiedliche Auffassungen. Der Auftragsverarbeiter ist jedenfalls gesetzlich verpflichtet, den Verantwortlichen bei der Einhaltung der Meldepflichten gegenüber Behörden und Betroffenen zu unterstützen und hat dazu alle erforderlichen Informationen über Sicherheitsverletzungen unverzüglich an den Verantwortlichen zu übermitteln. Ein Auftragsverarbeiter, der eine Sicherheitsverletzung zunächst intern aufarbeitet und den Auftraggeber erst nach mehreren Tagen oder Wochen informiert, würde nicht nur vertragswidrig handeln, sondern auch gegen ihn selbst betreffende gesetzliche Vorgaben verstoßen und sich damit erheblichen Bußgeldrisiken aussetzen.

Die Kenntnis einer Datenschutzverletzung wird dem Auftraggeber spätestens von dem Zeitpunkt an zugerechnet, an dem ein Mitarbeiter des Auftraggebers durch Information des Auftragsverarbeiters davon erfährt. Es ist daher durch entsprechende Verfahren sicherzustellen, dass sämtliche Mitteilungen des Auftragsverarbeiters immer und unmittelbar auch den für Datenschutzverletzungen intern zuständigen Stellen zugehen.

Bereits bei der Gestaltung des Auftragsverarbeitungsvertrages können geeignete Vorkehrungen getroffen werden, um den o. g. Herausforderungen zu begegnen. Denkbar sind etwa die Festschreibung interner Meldefristen, Klauseln zur Einbeziehung von externen Sicherheitsexperten sowie die ausdrückliche Vereinbarung von Kommunikationswegen.

Dokumentationspflichten und Lessons learned

Als Ausformung der allgemeinen Rechenschaftspflicht bestimmt Art. 33 Abs. 5 DSGVO eine Dokumentationspflicht bei Sicherheitsverletzungen. Diese Pflicht bezieht sich auch auf Sicherheitsverletzungen, die vom Verantwortlichen als nicht meldepflichtig eingestuft wurden, da diese im Zweifel der Kontrolle durch die Aufsichtsbehörden unterliegen.

Mit der etwaigen Meldung, der Ursachenbehebung und Dokumentation des Vorgangs ist es jedoch noch nicht getan. Die DSGVO verlangt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Die aufgetretenen Defizite sind daher als Anlass zu nehmen, um im Rahmen des geforderten kontinuierlichen Verbesserungsprozesses die Wirksamkeit der Schutzmaßnahmen im betroffenen und in ähnlichen Verarbeitungsverfahren zu prüfen. Unternehmen, die über ein funktionierendes Informationssicherheitsmanagementsystem >

(ISMS) verfügen, können diese Prüfungshandlungen in Abstimmung mit dem Datenschutzbeauftragten in den bereits etablierten Verbesserungsprozess (PDCA) einsteuern. In Unternehmen ohne ISMS kann die Prüfung durch den Datenschutzbeauftragten erfolgen. Dieser hat der Datenschutzverletzung ohnehin Rechnung zu tragen und seinen Prüfplan entsprechend anzupassen.

Auch die bei der Bearbeitung der Sicherheitsverletzung gewonnenen Erkenntnisse über die Angemessenheit und Wirksamkeit der Data-Breach-Management-Prozesse sollten im Rahmen von „Lessons learned" regelmäßig ausgewertet werden, um deren Effektivität messen und verbessern zu können.

Zu beteiligende Stellen

Unternehmen sollten die Zuständigkeiten und Verfahrensweisen für die Erkennung, Bewertung, Umsetzung von Nachsorgemaßnahmen und die Dokumentation von Datenschutzverletzungen (Data-Breach-Management) als Teil des Gesamtprozesses für das Management von Informationssicherheitsvorfällen festlegen.

Ein Informationssicherheitsvorfall sollte innerhalb der vorhandenen Prozesse und Verfahren demnach immer auch dahingehend bewertet werden, ob es sich dabei um eine Datenschutzverletzung handeln könnte. Darüber hinaus sollte in Anlehnung an erprobte Verfahren aus dem Notfallmanagement für die Bewältigung von Datenschutzverletzungen eine geeignete „Bewältigungsorganisation" in Form eines Teams oder Ausschusses mit verschiedenen Rollen bestimmt werden. Dieses kann je nach Art, Umfang und Schwere der Datenschutzverletzung aktiviert und in unterschiedlicher Konstellation temporär zusammengesetzt werden.

Das Kernteam zur Behandlung der Datenschutzverletzung sollte mindestens aus dem Leiter der betroffenen Organisationseinheit bzw. einem Bereichsverantwortlichen, dem Datenschutz-Referenten (alternativ dem Datenschutzmanager, Datenschutzspezialisten oder Datenschutzkoordinator), einem Vertreter des IT-Betriebs, dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten bestehen.

Dem Leiter der betroffenen Organisationseinheit kommt dabei eine zentrale Rolle zu. Ihm obliegt die Risikobewertung ebenso wie die Entscheidung über die Durchführung einer Meldung bei der Aufsichtsbehörde und die Benachrichtigung der Betroffenen. Unterstützt wird er in erster Linie vom Datenschutz-Referenten (in kleineren Unternehmen vom Datenschutzkoordinator, bei Kleinstunternehmen vom Datenschutzbeauftragten). Kommt der Leiter der Organisationseinheit zu dem Bewertungsergebnis, dass voraussichtlich kein Risiko besteht, so hat er dennoch sicherzustellen, dass sämtliche Informationen zum Vorgang dokumentiert und dem Datenschutzbeauftragten zur Verfügung gestellt werden.

Für den Datenschutzbeauftragten sehen weder die DSGVO noch das BDSG Aufgaben im Rahmen der Behandlung von Datenschutzvorfällen vor. Gleichwohl ist es möglich und überdies sinnvoll, den Datenschutzbeauftragten in alle Beratungen und Entscheidungen einzubinden. Dabei ist jedoch zu beachten, dass er gem. Art. 38 Abs. 3 DSGVO stets unabhängig und weisungsfrei agiert. Aufgaben, die zu einem Interessenkonflikt führen könnten, dürfen ihm nicht delegiert werden. Mithin darf ihm die Zuständigkeit für die Umsetzung und Einhaltung datenschutzrechtlicher Vorschriften nicht übertragen werden.

Den Datenschutzbeauftragten mit der Durchführung der Sachverhaltsermittlung und Risikoermittlung zu beauftragen, ist demnach unzulässig. Allenfalls die Aufgabe zur Meldung an die Aufsichtsbehörde kann an ihn delegiert werden (die Entscheidung über die Meldung darf er jedoch nicht selbst treffen). Zulässig ist es zudem, dass der Datenschutzbeauftragte um eine Stellungnahme und Einschätzung zu der vom Leiter der betroffenen Organisationseinheit angefertigten Risikoprognose gebeten wird, da dies Bestandteil seines Beratungsauftrages ist.

Je nach Art und Ausmaß der Datenschutzverletzung können zum Team weitere Stellen hinzugezogen werden. Dazu zählen beispielsweise der Notfallbeauftragte, der Compliance-Officer, der IT-Leiter, das Justitiariat, die Personalabteilung (sofern die Datenschutzverletzung auf das Fehlverhalten eines Beschäftigten zurückgeht), die Presse-/Öffentlichkeitsabteilung (für eine kommunikativ versierte Begleitung) und die Arbeitnehmervertretung (soweit Mitarbeiterdaten betroffen sind).

Fazit

Bei Datenschutzverletzungen ist besonders schnelles Handeln gefragt.

Bei Verzögerungen drohen hohe finanzielle und reputative Risiken. Unternehmen müssen daher Prozesse zur Behandlung von Datenschutzverletzungen sinnvoll in bestehende Strukturen eingliedern und mit bereits bestehenden Managementsystemen synchronisieren. Soweit etwaige Meldepflichten aus anderen Regulierungen und Normen gelten (zu denken ist hier etwa an das BaFin-Rundschreiben zur Meldung schwerwiegender Zahlungssicherheitsvorfälle, an § 8b Abs. 4 BSIG oder an sonstige zivilrechtliche Meldepflichten), sind sie diese dabei ebenfalls zu berücksichtigen.

Verantwortliche, die es fahrlässig unterlassen, ein Data-Breach-Management (welches auch die Sensibilisierung von Mitarbeitern umfasst) zu implementieren und damit für schnelle Informationswege und kurze Bearbeitungszeiten zu sorgen, müssen sich ein Organisationsverschulden vorwerfen lassen und riskieren die Verwirklichung gleich mehrerer Bußgeldtatbestände.

Sind entsprechende Prozesse einmal vorhanden, kann auch ein im Einzelfall nachlässiger Umgang mit personenbezogenen Daten durch eine sorgfältige und entschlossene Aufarbeitung sowohl der Öffentlichkeit als auch der zuständigen Aufsichtsbehörde gegenüber als singulärer und gleichwohl positiver Vorgang dargestellt werden, welcher zudem den eigenen Kunden zeigt, wie wichtig die Einhaltung des Datenschutzes dem betroffenen Unternehmen ist. ▬

AUTOR UND ANSPRECHPARTNER

Maximilian Schmidt
Beauftragter Informationssicherheit und Datenschutz
E-Mail: maximilian.schmidt@dz-cp.de

▶ **Datenschutz**

EDSA-Leitlinie zum Auskunftsersuchen

AUTORIN UND ANSPRECHPARTNERIN

Claudia Gerst
Analystin Informationssicherheit & Datenschutz
E-Mail: claudia.gerst@dz-cp.de

Im Januar dieses Jahres hat der Europäische Datenschutzausschuss (EDSA) seine Leitlinie zum Auskunftsrecht veröffentlicht. Das Auskunftsrecht gem. Art. 15 DSGVO ist eines der grundlegendsten und in der Praxis wohl meistgenutzten Betroffenenrechte, das die DSGVO enthält. Zwar steht dieses Instrument betroffenen Personen schon lange zur Verfügung, über seine Reichweite herrschte bis-her jedoch Uneinigkeit. Mit der neuen Leitlinie sorgt der Europäische Datenschutzausschuss nun für mehr Klarheit und stärkt gleichzeitig die Rechte der Betroffenen.

Rechte der Betroffenen stehen an erster Stelle

Mit der neuen Leitlinie stellt der Europäische Datenschutzausschuss eines klar: Die Rechte der betroffenen Personen stehen an erster Stelle. Wie zu erwarten war, vertritt der Europäische Datenschutzausschuss eine weite Auslegung des Auskunftsanspruchs, um es den Betroffenen möglichst einfach zu machen, ihre Rechte in Anspruch zu nehmen und die Informationen über ihre personenbezogenen Daten zu erhalten. Dies führt jedoch im Umkehrschluss dazu, dass Unternehmen sich weiterhin auf einen nicht unerheblichen Aufwand einstellen müssen und nur wenige Fälle bleiben, in denen sie Auskunftsersuche abweisen können. So ist ein hoher Bearbeitungsaufwand für das Unternehmen oder die mögliche Motivation des Betroffenen kein Grund mehr, um dem Auskunftsersuchen nicht nachzukommen.

Auch über die formellen Anforderungen macht der Europäische Datenschutzausschuss Angaben: Betroffene können formlos und ohne Angabe von Gründen ihr Anliegen an den Verantwortlichen senden. Nur Anfragen, die an eine vollkommen willkürliche und offensichtlich unrichtige Adresse gesendet werden (z.B. an die Adresse des Reinigungspersonals), können unbeachtet bleiben.

Weiter haben Betroffene das Recht, eine vollständige Kopie ihrer gespeicherten Daten zu erhalten, nicht nur eine grobe Zusammenfassung. Dabei ist es wichtig, nicht nur die elektronisch gespeicherten Daten zu beauskunften, sondern auch solche, die papierhaft vorliegen. Auch unrichtige Daten sowie möglicherweise unrechtmäßig verarbeitete Daten müssen dem Betroffenen zur Verfügung gestellt werden. Daten, die beispielsweise aufgrund von Aufbewahrungspflichten bereits gelöscht sind, sind nicht mitzuteilen.

Bei der Beantwortung der Anfrage, also der Mitteilung der verarbeiteten Daten, ist darauf zu achten, dass Sie als Unternehmen einen sicheren Übertragungsweg wählen. Dies kann eine verschlüsselte E-Mail, eine verschlüsselte Datei, ein Portal mit verschlüsselter Übertragung oder der Postweg sein. Werden die Daten der betroffenen Person nicht geschützt, so kann hieraus ein meldepflichtiger Datenschutzvorfall resultieren, den es zu vermeiden gilt.

Was sollten Unternehmen tun?

Unternehmen sollten die Aussagen des Europäischen Datenschutzausschusses nutzen, um ihre internen Prozesse zur Bearbeitung von Auskunftsersuchen zu überarbeiten und ihre Mitarbeiter bezüglich des Themas zu sensibilisieren. Klar definierte Zuständigkeiten, Textvorlagen und Abläufe erleichtern den Prozess und ermöglichen eine effizientere Bearbeitung.

Leitlinien des Europäischen Datenschutzausschusses sind nicht rechtsverbindlich. Sie stellen „lediglich“ die Auffassung der Datenschutzbehörden dar. Die Empfehlungen nicht oder nicht vollständig umzusetzen hat somit keine direkten negativen Auswirkungen in Form von Bußgeldern oder Ähnlichem. Mit Einhaltung dieser Leitlinien ist jedoch ein aufsichtsbehördliches Verfahren sehr unwahrscheinlich. ▬

Informationssicherheit

Umgang mit Cybercrime

Wirtschaftsunternehmen stehen weiterhin weltweit im Fokus von Cyberkriminellen. Deren Ziel ist es, Daten, Knowhow und Informationen auszuspähen bzw. zu stehlen oder die Unternehmen zu erpressen, indem sie mit „Distributed Denial of Service"– sinngemäß Serverüberlastung – drohen. Daneben stellen auch unspezifische, breit gestreute Angriffe (Ransomware) eine hohe Gefahr für die IT-Infrastruktur dar.

Cybercrime umfasst alle illegalen Aktivitäten, die über einen Computer oder ein ähnliches internetfähiges Gerät ausgeführt werden. Angriffsziele sind hierbei meistens Unternehmen. Mittelbar findet hierdurch jedoch auch ein Angriff auf Verbraucher, beispielsweise durch Datenklau, statt.

Die Absichten sind immer gleich: Schaden verursachen und Geld verdienen, z. B. durch einen Zugriff auf Finanzkonten, indem unter fremden Namen Dienstleistungen in Anspruch genommen werden, Dateien gesperrt oder persönliche Daten für Erpressungen abgegriffen werden.

Kritische Bedrohungslage durch Log4j

Einer der bedeutendsten Cybervorfälle, die in jüngster Zeit bekannt wurden, betraf Apaches Log4j. Die in der Java-Bibliothek entdeckte Schwachstelle führte Mitte Dezember 2021 zu einer kritischen Bedrohungslage.

Log4j ist eine Software, die als Logging Framework verwendet wird, d. h, sie ermöglicht Entwicklern die Überwachung bzw. Protokollierung digitaler Ereignisse auf einem Server. Auf der ganzen Welt wird diese Bibliothek aufgrund ihrer Funktionalität von Programmierern und Systemadministratoren in Rechenzentren in ihre Unternehmensservern, Netzwerkkomponenten und Systemkomponenten eingebunden. Durch die Protokolle lässt sich überprüfen, ob der Betrieb regulär abläuft oder es Anzeichen für ein abnormales Verhalten gibt.

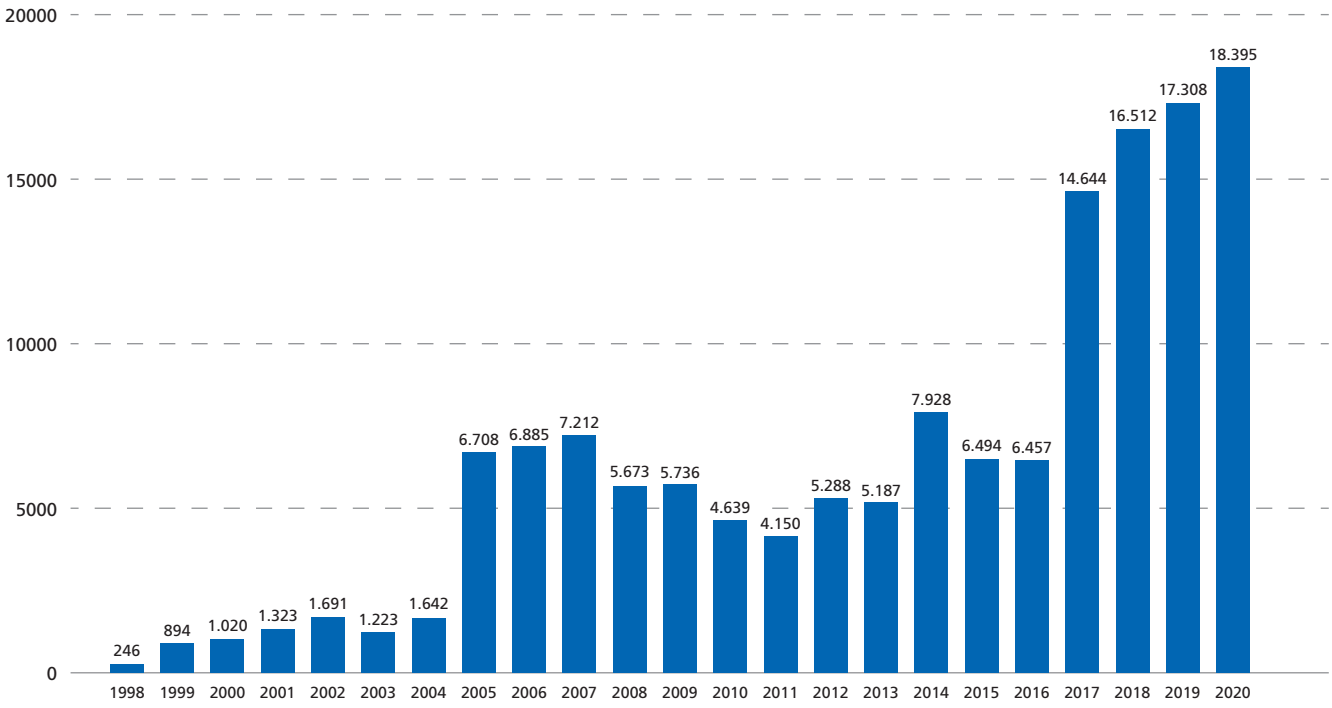
Im aktuellen Fall gestattete ein Fehler nicht autorisierten Benutzern einen ersten Zugang, mit dem sie auf sensible Daten zugreifen und sogar die Servereinstellungen manipulieren konnten. Dies führte zur potenziellen Verwundbarkeit von mehreren Milliarden Computern. Das bedeutete auch, dass Produkte zahlreicher Internetkonzerne schwerwiegende Sicherheitslücken aufwiesen und zeitweise als unsicher galten.

Zwar wurden Updates zwischenzeitlich bereitgestellt. Doch haben nicht alle Dienstebetreiber und Softwareentwickler die nötigen Aktualisierungen vorgenommen, sodass die entsprechenden Systeme weiterhin verwundbar sein können. Zusätzlich zum Update verlangt die gegenwärtige Lage, dass die Systeme und Server nach dem Update auf Unregelmäßigkeiten geprüft werden.

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) rechnen Expertinnen und Experten mit langfristigen negativen Folgen für Unternehmen jeder Größe. Kriminelle könnten die Zeit genutzt haben, um Backdoors und Brückenköpfe zu installieren. Bleiben diese unentdeckt, können sie genutzt werden, um das System/die Daten im Nachgang z. B. auszuspähen, zu manipulieren und/oder zu verschlüsseln. Besteht der Verdacht, dass z. B. Schadsoftware eingeschleust wurde, sollten Betroffene auf bestehende Sicherungskopien zurückgreifen.

Durch die bereitgestellten Updates hat das BSI die Warnstufe von Rot auf Orange herabgesetzt. Das bedeutet jedoch nicht automatisch eine Entwarnung für das einzelne Unternehmen. So banal es klingt: Die Unternehmen müssen sich des Risikos weiter bewusst sein und entsprechend handeln. >

ABB. 1 ANZAHL SCHWACHSTELLEN IN COMPUTERSYSTEMEN NACH KALENDERJAHREN



Anzahl an veröffentlichten Software-Schwachstellen basierend auf zugewiesenen CVE-Nummern (Common Vulnerabilities and Exposures; Standard zur Benennung von Sicherheitslücken in Computersystemen)
Quelle der Grafik: Bundeskriminalamt (BKA)

Patchmanagement – der Weg zu mehr Überblick

Die Anzahl neu entwickelter Schadprogramme wird sich auf hohem Niveau weiterentwickeln. Auch wird sich die Zahl der betroffenen Unternehmen erhöhen. Angriffsszenarien, die regelmäßig bekannt werden, zeigen immer wieder, wie wichtig es ist, die eingesetzte Hard- und Software durch Sicherheits-Updates vor solchen Angriffen zu schützen.

Viele Unternehmen sind jedoch in puncto Updates nicht auf dem neuesten Stand. Trotz der Tatsache, dass Softwarehersteller bemüht sind, fehlerfreie und sichere Programme zu veröffentlichen, sind während des gesamten Produktzyklus Aktualisierungen und Patches erforderlich.

Patches (deutsch Flicken) sind Softwarepakete, mit denen die Hersteller Sicherheitslücken in ihren Programmen schließen. Sie beheben u. a. Programmfehler und verhindern so den Erfolg von Malware-Angriffen (bösartige Software). Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt daher schnell zu möglichen Angriffspunkten.

In den meisten Unternehmen besteht die IT-Infrastruktur aus einer Mischung älterer wie auch aktueller Technologien. So laufen zum Teil verschiedene Betriebssysteme auf Endpoints und Servern im Netzwerk. Hier werden wiederum Hunderte von geschäftlichen Anwendungen abgebildet, die auf Änderungen im Betriebssystem unterschiedlich reagieren. Sind diese schlecht oder gar nicht gepatcht, bieten sie ein Einfallstor für Angreifer.

Ein zentrales und regelmäßiges Patchmanagement sichert die Einhaltung von Compliance-Regeln und erleichtert die einfache und schnelle Verteilung von Patches.

Um die Ordnung im System zu erhalten, ist es notwendig, eine Übersicht über alle Endpoints im Netzwerk – also Laptops, Desktops, Server und weitere Geräte sowie die darauf installierte Software – zu erstellen. Idealerweise umfasst die Inventarisierung auch die auf den Systemen

AUTORIN UND ANSPRECHPARTNERIN

Katja Schlüter
Beauftragte Informationssicherheit und Datenschutz
E-Mail: katja.schlueter@dz-cp.de

installierten Softwareversionen und Softwarelizenzen. Zudem erleichtert eine einheitliche IT-Umgebung die Kontrolle über installierte Softwareprodukte.

Durch ein wirkungsvolles Patchmanagement soll sichergestellt werden, dass Patches zeitnah ausgerollt werden, um Sicherheitslücken erkennen, klassifizieren und beheben zu können:

- Sind Informationen bereitgestellt, sollten die Updates bewertet werden und sollte geprüft werden, ob und wann die Patches installiert werden.
- Speziell bei Clientsoftware ist es empfehlenswert, die Patches vor ihrer Verteilung in einer Testumgebung zu installieren, um möglichen Kompatibilitätsproblemen vorzubeugen.
- Schlussendlich ist das Sammeln von Informationen die Basis für ein angemessenes und wirkungsvolles Patchmanagement. Dabei können Informationen von Drittanbieterquellen, wie entsprechende Informationswebseiten von Herstellern, oder unter www.cert-bund.de abonniert werden.

Ohne ein Patch kann ein Angreifer Sicherheitslücken nutzen, um Serveranwendungen und angeschlossene Geräte fremdzusteuern und Unternehmensnetzwerke zu infiltrieren.

All das Vorgesagte gilt natürlich auch für Computersysteme, die von Privatpersonen genutzt werden.

Im Falle einer Rechnerinfizierung bleibt den Betroffenen nur noch die – hoffentlich funktionierende – Recovery (Wiederherstellungsprozedur) und der Rückgriff auf eine – hoffentlich umfassende – Datensicherung, um an einem Restart-Point vor der Infizierung aufsetzen zu können.

Fazit

Wer der regelmäßigen Durchführung von Patch-Updates zu wenig Bedeutung beimisst, geht ein unkalkulierbares und hohes Risiko für sein Unternehmen ein. Tagtäglich arbeiten Hacker und Cyberkriminelle daran, Sicherheitslücken in viel genutzten Anwendungen zu finden und für ihre Zwecke zu missbrauchen.

Die Methoden der Cyberangriffe entwickeln sich laufend weiter. Die Konzeption und Implementierung von Schutzmöglichkeiten dagegen können dieser Entwicklung nur mit einer entsprechenden Verzögerung folgen. Um ein jederzeit ausreichendes Schutzniveau aufrechtzuerhalten, muss die Risikoabschätzung zyklisch wiederholt und die IT-Sicherheitslösung ggf. angepasst werden.

IT-Sicherheit stellt somit keinen statischen Zustand dar, sondern muss als ein ständiger Regelkreislauf bzw. andauernder Prozess verstanden werden. ▬

Geldwäsche- und Betrugsprävention

Sanktions- und Embargobestimmungen

Die politischen Entwicklungen der vergangenen Monate haben dem Thema „Sanktions- und Embargobestimmungen" zu (leider) hoher Aktualität verholfen. Wir geben in diesem Artikel einen Überblick über die Zusammenhänge rund um diesen Themenkomplex.

Sanktions- und Embargobestimmungen können gegenüber Ländern, einzelnen Personen, Unternehmen, Organisationen und speziellen Wirtschaftsbereichen verhängt werden.

Aktuelle Beispiele auf zwischenstaatlicher Ebene sind die bereits seit Längerem bestehenden Embargo- und Sanktionsmaßnahmen gegen Iran und Nordkorea sowie die seit Februar 2022 verabschiedeten Sanktions- und Embargobestimmungen gegen Russland und Belarus.

Durch Embargo- und Sanktionsmaßnahmen sollen völkerrechtswidriges Verhalten oder die Bedrohung der internationalen Sicherheit bestraft und die sanktionierten Staaten zu einem Umdenken veranlasst werden.

Begrifflichkeiten

Mit einem Embargo (spanisch: „Beschlagnahme, Pfändung") soll der Im- bzw. Export von Waren oder Rohstoffen in ein bzw. aus einem bestimmten Land unterbunden werden.

Embargos werden gegen ein bestimmtes Land ausgesprochen, um dieses beispielsweise von Import und Export abzu-spalten. In der Folge bekommt dieses Land häufig wirtschaftliche Probleme mit nachgelagerten innenpolitischen Auswirkungen.

Der UN-Sicherheitsrat verwendet Embargos oder andere Sanktionen als Druckmittel gegen Länder, die gegen das Völkerrecht verstoßen.

Finanzsanktionen beschränken den Kapital- und Zahlungsverkehr. Sie stehen meist im Zusammenhang mit restriktiven Maßnahmen, die sich direkt gegen einzelne Personen, Einrichtungen oder Organisationen richten. Beispiele sind Maßnahmen gegen einzelne Mitglieder der Regierung oder exponierte Wirtschaftsfunktionäre („Oligarchen") eines vom Embargo betroffenen Landes oder auch Embargomaßnahmen, die zur Bekämpfung des Terrorismus verabschiedet wurden.

Durch die Finanzsanktionen wird in der Regel das Vermögen der betroffenen Personen eingefroren. Auch dürfen diesen Personen keine Gelder oder sonstige **wirtschaftliche** Ressourcen mehr zur Verfügung gestellt werden. Teilweise sind Ausnahmen nach vorheriger Genehmigung möglich.

- **Gelder** umfassen dabei finanzielle Vermögenswerte oder wirtschaftliche Vorteile jeder Art einschließlich – aber nicht beschränkt auf – Bargeld, Schecks, Geldforderungen, Wechsel, Geldanweisungen oder andere Zahlungsmitteln, Guthaben bei Finanzinstituten oder anderen Einrichtungen. Das Einfrieren soll jegliche Form von Bewegungen, Transfers, Veränderungen, Verwendung von Geldmitteln und den Handel mit ihnen verhindern.
- **Wirtschaftliche Ressourcen** stellen Vermögenswerte jeder Art dar, die keine Gelder sind oder für deren Erwerb verwendet werden können, unabhängig davon, ob sie materiell oder immateriell und beweglich oder unbeweglich sind. Beim Einfrieren wird verhindert, dass sie für den Erwerb von Geldern, Waren oder Dienstleistungen verwendet werden. Dies schließt auch den Verkauf, das Vermieten oder das Verpfänden von ihnen ein.

Sanktionslisten sind offizielle Verzeichnisse, in denen Personen, Gruppen, Organisationen oder Wirtschaftsgüter (Waren) aufgeführt sind, gegen bzw. für die wirtschaftliche und/oder rechtliche Einschränkungen ausgesprochen wurden.

- Während die **personen-/organisationsbezogenen Sanktionslisten** der weltweiten Terrorismusbekämpfung und der Unterstützung von Embargos dienen,

- werden die **güterbezogenen Sanktionslisten** aus politischen und/oder wirtschaftlichen Gründen (z. B. Einfuhrzölle auf bestimmte in einer Sanktionsliste aufgeführte Produkte) erlassen.

Eine der wesentlichen Rechtsgrundlagen ist in diesem Zusammenhang das **Außenwirtschaftsgesetz (AWG).**

Das AWG dient dem Schutz von Allgemeinwohlinteressen, vor allem im außen- und sicherheitspolitischen Sinne. Es enthält größtenteils Blankettvorschriften, die auf Ausfüllungsnormen mit den entsprechenden Beschränkungen verweisen. Letztere ergeben sich regelmäßig aus der Außenwirtschaftsverordnung (AWV).

Das nationale Außenwirtschaftsrecht wird jedoch häufig durch vorrangiges Gemeinschaftsrecht und internationales Recht überlagert.

Verstöße gegen Finanzsanktionsrechtsakte können nach dem Außenwirtschaftsgesetz (AWG) und der Außenwirtschaftsverordnung (AWV) als Ordnungswidrigkeit (§ 19 AWG) und in bestimmten Fällen auch als Straftat (§§ 17 und 18 AWG) geahndet werden.

Embargos

Nach traditionellem Verständnis sind Embargos Wirtschaftssanktionen, die gegenüber einem bestimmten Staat verhängt werden. Der Außenwirtschaftsverkehr mit diesem Staat wird nach Maßgabe des entsprechenden Embargos eingeschränkt oder sogar komplett untersagt.

Ein typisches Beispiel für ein Embargo ist das Verbot, Rüstungsgüter in einen bestimmten Staat auszuführen (Waffenembargo). Embargomaßnahmen können aber je nach Zielsetzung auch einzelne politische Gruppierungen oder Individuen sowie unterschiedliche Wirtschaftsbereiche betreffen und dementsprechend eine unterschiedliche Tragweite haben.

Embargos gehen als spezialgesetzliche Regelungen den allgemeinen Beschränkungen im Außenwirtschaftsverkehr vor, wie sie z. B. durch die Verordnung (EG) Nr. 1334/2000 (EG-Dual-Use-Verordnung) oder das AWG bzw. die AWV begründet werden.

- Mit der EG-Dual-Use-Verordnung hat die EU für alle EU-Mitgliedsstaaten gemeinsame Genehmigungspflichten und Verfahrensweisen bei der Ausfuhr von Gütern mit doppeltem Verwendungszweck festgelegt.
- Als Güter mit doppeltem Verwendungszweck gelten Gegenstände, Technologien und Kenntnisse, die i. d. R. zivilen Zwecken dienen, die aber auch für militärische Zwecke verwendet werden können (z. B. kerntechnische Materialien, Anlagen und Ausrüstung, Werkstoffe, Chemikalien, Mikroorganismen und Toxine, allgemeine Elektronik, Telekommunikations- und Informationssicherheitstechnik, Sensoren und Laser, Luftfahrtelektronik und Navigation, Antriebssysteme, Raumfahrzeuge und zugehörige Ausrüstung etc.).

Embargos gehen meist auf Beschlüsse internationaler Organisationen zurück, vor allem auf Resolutionen des Sicherheitsrates der Vereinten Nationen (VN). Aber auch Beschlüsse der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) können Grundlage eines Embargos sein. Diese Beschlüsse im Rahmen internationaler Organisationen binden die Mitgliedsstaaten völkerrechtlich. Damit diese Beschlüsse eine unmittelbare rechtliche Geltung entfalten, bedarf es weiterer Rechtsakte auf europäischer und/oder nationaler Ebene.

In der EU werden Embargomaßnahmen von den EU-Mitgliedsstaaten im Rahmen der gemeinsamen Außen- und Sicherheitspolitik vereinbart, und zwar in der Regel im Wege eines „Gemeinsamen Standpunktes“ nach Art. 15 EU-Vertrag. Die meisten „Gemeinsamen Standpunkte“, die im Zusammenhang mit Embargomaßnahmen angenommen wurden, entsprechen vorausgegangenen Beschlüssen des Sicherheitsrates der Vereinten Nationen.

Es ist aber auch möglich, dass die EU eigene, unabhängige Sanktionen verhängt. Für die Bürgerinnen und Bürger und Unternehmen entfalten diese Standpunkte genau wie die Resolutionen des UN-Sicherheitsrates zunächst keine unmittelbare Rechtswirkung.

Wie die Umsetzung des Embargos in unmittelbar bindendes Recht erfolgt, entscheidet sich nach dem Gegenstand der Embargomaßnahme. Grundsätzlich betreffen Embargomaßnahmen den Außenhandel der Europäischen Gemeinschaft. Insofern ist eine Zuständigkeit der EG prinzipiell gegeben. Für den Bereich der Wirtschaftssanktionen setzt die EG die „Gemeinsamen Standpunkte“ in unmittelbar geltende EG-Verordnungen um.

Es gibt jedoch Bereiche, die von der Zuständigkeit der Europäischen Gemeinschaft ausgenommen sind. >

Hierzu zählt der Handel mit Waffen und Rüstungsgütern. Insofern werden die in den „Gemeinsamen Standpunkten" vorgesehenen Waffenembargos nicht durch EG-Verordnungen umgesetzt, sondern durch nationalstaatliche Regelungen, in Deutschland beispielsweise durch die Außenwirtschaftsverordnung (§§ 74 ff. AWV).

Die mit Embargos verbundenen Beschränkungen können sowohl nach dem Umfang der einzelnen Maßnahmen als auch nach den betroffenen Wirtschaftsbereichen/Tätigkeiten unterschieden werden.

Hinsichtlich des Umfangs der Beschränkungen lässt sich zwischen Totalembargos und Teilembargos unterscheiden.

- Totalembargos verbieten jeglichen Handel mit dem oder zugunsten des Adressaten.
- Teilembargos zählen ebenfalls zu den länderbezogenen Embargos. Sie können eine unterschiedliche Tragweite haben. Einerseits können Beschränkungen des Kapital- und Zahlungsverkehrs einschließlich eines Verbots der Bereitstellung von wirtschaftlichen Ressourcen angeordnet werden, andererseits aber auch darüber hinausgehende Maßnahmen, z. B. Beschränkungen des Reiseverkehrs oder Einschränkungen des Handels mit bestimmten Gütern.

Teilembargos kombinieren die Beschränkungen zum Teil mit personenbezogenen Elementen, die dann nur gegenüber diesen bestimmten Personen gelten.

Weiterhin sind die verschiedenen Embargomaßnahmen nach den betroffenen Wirtschaftsbereichen bzw. Tätigkeiten zu unterscheiden. Hierzu zählen Waffenembargos, sonstige Ausfuhrverbote/-beschränkungen, das Verbot technischer und finanzieller Hilfe, Einfuhrverbote, Erfüllungsverbote, Reisebeschränkungen, Finanzsanktionen und Ausnahmetatbestände.

Waffenembargos zählen grundsätzlich zu den länderbezogenen Embargos. Sie betreffen die Rüstungsgüter des Teils I Abschnitt A der „Ausfuhrliste" und verbieten i. d. R. deren Verkauf und Ausfuhr in das jeweilige Land. Die „Ausfuhrliste" ist eine Anlage zum AWG und zur AWV, die eine Aufzählung von Waren enthält, deren Ausfuhr genehmigungsbedürftig ist.

Von Exportbeschränkungen im Rahmen von Embargomaßnahmen kann aber auch jede andere Art von Gütern betroffen sein. Bei Güterembargos wird im Gegensatz zur „Standard-Exportkontrolle" nicht zwingend auf deren Erfassung in den entsprechenden Exportkontrolllisten oder auf deren Verwendung für militärische oder kerntechnische Zwecke abgestellt.

Vielmehr enthalten diese Güterembargos zumeist eigene Listen oder detaillierte Beschreibungen der betroffenen Waren oder Warengruppen.

Eine wichtige Untergruppe von Güterembargos sind die Restriktionen hinsichtlich der Ausfuhr von Ausrüstung, die von dem sanktionierten Staat zur internen Repression seiner Bevölkerung eingesetzt werden kann. Erfasst sind hier bspw. Wasserwerfer, Bandstacheldraht, spezielle Fahrzeuge für den Gefangenenabtransport etc.

Besonders im Zusammenhang mit Waffenembargos und sonstigen Güterembargos ist zu beachten, dass meistens nicht nur der Verkauf und die Ausfuhr untersagt sind. Auch technische und finanzielle Hilfe, also die Bereitstellung der diesbezüglichen technischen Unterstützung sowie die Bereitstellung von Finanzmitteln, Finanzhilfen und Finanzdienstleistungen für deren Lieferung, ist regelmäßig verboten.

Zur begrifflichen Klarstellung sei angemerkt, dass technische Hilfe nach dem Verständnis des europäischen Gesetzgebers Folgendes umfasst: Montage, Erprobung, Wartung oder jede andere technische Dienstleistung; technische Hilfe kann in Form von Anleitung, Beratung, Ausbildung, Weitergabe von praktischen Kenntnissen oder Fertigkeiten oder in Form von Beratungsdiensten erfolgen und schließt auch Hilfe in verbaler Form ein.

Genauso können Embargovorschriften ein Importverbot für bestimmte Güter oder Güterklassen vorsehen (bspw. Rohdiamanten oder Hölzer).

Embargos sehen i.d.R. keine Ausnahmen für die Erfüllung bereits vor Inkrafttreten geschlossener Verträge oder entstandener Ansprüche vor (sogenannte Erfüllungsverbote). Daher sind Wirtschaftsunternehmen in der Gemeinschaft und in Drittländern dem Risiko von Schadensersatzansprüchen aus den betroffenen Ländern ausgesetzt, insbesondere nach der Aufhebung von Embargos.

Um Wirtschaftsunternehmen auf Dauer gegen solche Ansprüche zu schützen und das vom Embargo betroffene Land daran zu hindern, einen Ausgleich für negative Folgen des Embargos zu erhalten, können Erfüllungsverbote angeordnet werden.

Diese Erfüllungsverbote verbieten einerseits die Erfüllung von Schadensersatzansprüchen von Vertragspartnern, die sich auf die Nichterfüllung von Verträgen wegen des Embargos stützen, und schützen andererseits davor, dass solche Ansprüche nach Aufhebung des Embargos in der EU durchgesetzt werden können.

Personenbezogene Embargomaßnahmen können auch Reisebeschränkungen enthalten. Den betroffenen Personen wird in diesem Fall die Einreise und ggf. die Durchreise verweigert.

Gemeinsam ist den derzeit geltenden Embargos, dass sie neben den angeordneten Verboten grundsätzlich auch Ausnahmen für bestimmte, in den Rechtsakten einzeln aufgeführte Sachverhalte vorsehen **(Ausnahmetatbestände).** Das heißt, in diesen Fällen können bei Vorliegen der Voraussetzungen Ausfuhrgenehmigungen erteilt werden.

Beispielsweise wird in der Regel die Belieferung von UN-Friedenstruppen mit Rüstungsgütern nicht von dem Waffenembargo erfasst sein, welches gegen das Land besteht, in dem die Blauhelmsoldaten eingesetzt sind.

Eine aktuelle Übersicht der länderbezogenen Embargos stellt das Bundesamt für Wirtschaft und Ausfuhrkontrolle regelmäßig bereit (https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Embargos/embargos_node.html).

Finanzsanktionen

Neben den länderbezogenen Embargos gibt es restriktive Maßnahmen, die sich direkt gegen einzelne Personen, Einrichtungen oder Organisationen richten und damit unabhängig vom Aufenthaltsort der betreffenden Personen gelten. Dies sind z. B. die Embargomaßnahmen der EG zur Bekämpfung des Terrorismus oder im Zusammenhang mit dem Krieg in der Ukraine.

Derartige personenbezogene Sanktionen können jedoch auch im Rahmen von länderbezogenen Embargoverordnungen vorgesehen sein (z. B. Maßnahmen gegen einzelne Mitglieder der Regierung des betroffenen Landes).

Inhaltlich enthalten die personenbezogenen Embargovorschriften zumeist Finanzsanktionen. Dadurch wird das Vermögen der betroffenen Personen eingefroren. Diesen Personen dürfen auch keine Gelder oder sonstige wirtschaftliche Ressourcen mehr zur Verfügung gestellt werden. Ausnahmen sind nach vorheriger Genehmigung möglich (siehe: https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/ausfuhrkontrolle_node.html).

Regelungsstruktur von Finanzsanktionen

Beschränkungen des Kapital- und Zahlungsverkehrs sind in Deutschland auf der Grundlage von Sanktionsmaßnahmen

- der Vereinten Nationen,
- der Europäischen Union,
- der nationalen Behörden

möglich.

Maßgeblich bestimmt werden derartige Beschränkungen vom EU-Recht. Danach gilt innerhalb der EU sowie im Verhältnis der EU zu Drittstaaten der Grundsatz der Kapital- und Zahlungsverkehrsfreiheit. Beschränkungen sind im Wesentlichen nur im Bereich von Finanzsanktionen zulässig.

Die durch **Resolutionen des Sicherheitsrats** der Vereinten Nationen verhängten Sanktionsmaßnahmen richten sich allein an Staaten und bedürfen der Umsetzung in den jeweiligen Rechtsordnungen.

In der Europäischen Union ist zur Umsetzung von Resolutionen des Sicherheitsrates der Vereinten Nationen zunächst ein Beschluss des Rates erforderlich. Diese Beschlüsse gelten nicht unmittelbar in den Mitgliedsstaaten, sondern bedürfen der Umsetzung. Diese erfolgt in der Regel durch EU-Verordnungen. Diese EU-Verordnungen gelten unmittelbar in jedem Mitgliedsstaat.

Sanktionsmaßnahmen der Europäischen Union sind auch ohne zugrunde liegende Maßnahmen der Vereinten Nationen möglich. Dazu ist zunächst wiederum ein Beschluss des Rates erforderlich, in dem der Standpunkt der EU zu einer bestimmten Frage bestimmt wird (Art. 29 EUV). Dieser wird in der Regel – wie auf Sanktionsmaßnahmen der Vereinten Nationen beruhende Beschlüsse – durch eine EU-Verordnung umgesetzt.

Daneben können die Mitgliedsstaaten in Ausnahmefällen bei Vorliegen schwerwiegender politischer Umstände aus Gründen der Dringlichkeit einseitige, nationale Sanktionsmaßnahmen auf dem Gebiet des Kapital- und Zahlungsverkehrs treffen, solange der (Minister-)Rat keine Maßnahmen getroffen hat. Diese (Eil-)Maßnahmen dienen in der Regel der zeitnahen Umsetzung von Sanktionsmaßnahmen und ergehen im Vorgriff auf Maßnahmen der Europäischen Union. Diese nationalen Beschränkungen werden regelmäßig nach Inkrafttreten entsprechender europarechtlicher Maßnahmen wieder aufgehoben.

Verstöße gegen Finanzsanktionen können – je nach Art des Embargos – als Ordnungswidrigkeit oder Straftat geahndet werden (§ 19 sowie §§ 17 und 18 AWG).

Einzelne Finanzsanktionen am Beispiel Terrorismusbekämpfung

Nach den Terroranschlägen vom 11. September 2001 wurden auch von der EU Sanktionslisten veröffentlicht, deren vorsätzliche Nichtbeachtung mit Freiheitsstrafen nicht unter zwei Jahren geahndet werden kann.

Hier bestehen derzeit mehrere Listen in Form von EU-Verordnungen, die ständig fortgeschrieben werden und über die Seite der Bundesbank abgerufen werden können.

Exemplarisch ist dabei die Liste 881/2002 (Al-Qaida- und Taliban-Liste) vom 27.02.2002 zu nennen, die seit Jahren regelmäßig fortgeschrieben und aktualisiert wird. Die EG-Sanktionsverordnungen gelten unmittelbar in jedem Mitgliedsland der EU.

Die EU-Sanktionsliste 881/2002 muss insbesondere bei Transaktionen beachtet werden. Das bedeutet, dass an niemanden, der auf dieser oder daran anschließenden Liste namentlich genannt wird, Geldmittel ausgegeben werden dürfen oder Geld von einer solchen Person angenommen werden darf. Gleichzeitig müssen alle Gelder der benannten Personen – soweit vorhanden – eingefroren werden.

Zusätzlich ist der Kundenbestand regelmäßig gegen diese (elektronisch bereitgestellten) Listen zu prüfen. Bei Kundenneuanlagen muss ebenfalls eine Prüfung gegen diese Listen (automatisiert) erfolgen.

Bei Transaktionen von Gelegenheitskunden (insbesondere bei Finanztransfergeschäften) sollte daher unabhängig von einem etwaigen Schwellenbetrag im GwG oder KWG immer eine Identifizierung des Kunden mittels gültigem Lichtbildausweis erfolgen.

Im Fall einer Übereinstimmung darf die Transaktion nicht ausgeführt werden. Es ist eine Verdachtsmeldung gem. § 43 GwG abzugeben; das Konto ist einzufrieren bzw. das Geld aus einer Transaktion muss einbehalten werden. Die Deutsche Bundesbank ist hierüber zu informieren.

Eine gezielte Namenssuche gelisteter Personen oder Organisationen ist über die Internetseite https://www.finanz-sanktionsliste.de/fisalis/ möglich.

AUTOR UND ANSPRECHPARTNER

Thomas Schröder
Abteilungsleiter Geldwäsche- und Betrugsprävention
E-Mail: thomas.schroeder@dz-cp.de

Bedeutung für den Finanzsektor

Der Finanzsektor ist verpflichtet, Kundenbestände mit den in den Sanktionslisten aufgeführten Adressen abzugleichen.

In diesem Zusammenhang sind der Listenabgleich bei Kundenneuanlage, die Transaktionsüberwachung und die Kundenbestandsprüfung wesentliche Eckpfeiler zur Einhaltung der Sanktionsbestimmungen. Die Pflege und Befüllung der in den Sanktionslisten enthaltenen Personen, Unternehmen bzw. sonstigen Institutionen wird durch die Atruvia® in den sogenannten (globalen) „Dow Jones"-Namenslisten Geno-SONAR® vorgenommen.

Bereits bei der Anlage eines Neukunden ist ein Abgleich im Bankenverfahren mit diesen einschlägigen Namenslisten möglich. Voraussetzung ist, dass die Genossenschaftsbank vor Ort das entsprechende Kennzeichen im agree-Bankenverfahren aktiviert („Prüfung auf Embargoliste im Dialog (BZ 7635)", Eingabewert = 1). Nutzt die Bank diese Option, ist die Gefahr einer Konto-Neueröffnung für eine sanktionierte Person oder Organisation praktisch ausgeschlossen.

Die Abwicklung des Zahlungsverkehrs der Kunden und damit die **Transaktionsüberwachung** des **Auslandszahlungsverkehrs** (Prüfung von ein- und ausgehenden Auslandszahlungen auf eine Sanktionsrelevanz bzw. sonstige Übereinstimmung mit den einschlägigen Sanktionslisten) übernimmt die DZ BANK AG für die über sie gerouteten Zahlungen. Im Falle einer Übereinstimmung wird die ein- bzw. ausgehende Zahlung nicht ausgeführt. Besonderheiten ergeben sich aufgrund der restriktiven Sanktionsbestimmungen gegen Belarus und Russland für Kunden der Genossenschaftsbanken derzeit bei der Durchführung von Zahlungen von und nach Russland bzw. Belarus. Neben der Finanztransaktionsprüfung wird bei allen Zahlungen mit warenwirtschaftlichem Bezug eine warenwirtschaftliche Prüfung durchgeführt (siehe hierzu auch die aktuellen Rundschreiben der DZ BANK AG). Die implementierten Prozesse werden durch die DZ BANK AG einer fortlaufenden Überprüfung unterzogen und ggf. angepasst.

Schließlich erfolgt eine tägliche **Prüfung des Kundenbestandes** der Genossenschaftsbank mithilfe des Monitoring-Programms Geno-SONAR®.

Unterstützung durch die DZ CompliancePartner GmbH

- Wir prüfen im Rahmen der Auslagerungsdienstleistung täglich mittels Geno-SONAR® den Kundenbestand unserer Kunden auf Übereinstimmungen mit den einschlägigen Sanktionslisten. Die Prüfung erfolgt dabei retrospektiv.
- Daneben prüfen wir mittels Geno-SONAR®, ob die in den Sanktionsrundschreiben der Deutschen Bundesbank genannten Personen, Unternehmen bzw. sonstigen Institutionen im Kundenbestand innerhalb des Primärbankverfahrens geführt werden, und informieren über das Ergebnis. Anschließend können unsere Kunden die entsprechende Meldung an die Bundesbank vornehmen.
- Im Falle einer Übereinstimmung entscheidet der in unserem Haus für die Bank zuständige Geldwäschebeauftragte über das weitere Vorgehen im Hinblick auf die Abgabe einer Verdachtsmeldung nach § 43 GwG. ▬

MaRisk-Compliance

Herausforderung Rechts-monitoring

Rechtsmonitoring ist aus dem Compliance-Alltag nicht wegzudenken und gehört zur täglichen Routine eines (MaRisk-)Compliance-Beauftragten. Bedenkt man, dass Stand Februar 2022 allein in Deutschland 1.733 Gesetze sowie 2.655 Rechtsverordnungen gelten und im Jahr 2021 an den Amts- und Landgerichten rund 1,1 Millionen zivilrechtliche Neueingänge zu verzeichnen waren, so ist die alles entscheidende Frage: Welche Regelungen und Entscheidungen sind von den Banken zu beachten und wie kann ein Überblick darüber geschaffen bzw. behalten werden?

Gesetzliche Voraussetzungen

Aus § 25a Kreditwesengesetz (KWG) in Verbindung mit AT 4.4.2 Mindestanforderungen an das Risikomanagement (MaRisk) ergibt sich für jedes Institut die Verpflichtung zur Einrichtung einer ordnungsgemäßen Geschäftsorganisation. Dies umfasst nach dem Gesetzeswortlaut auch die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen. Um die Einhaltung der zu beachtenden Regelungen zu gewährleisten, müssen diese Regelungen dem Institut bekannt sein. Dies umfasst auch etwaige Veränderungen schon bestehender Regelungen sowie die Kenntnisnahme neu hinzutretender Regelungen. Ein Rechtsmonitoring ist zwingend zu implementieren, um die Informationen beherrschen zu können. Ziel ist es also, das Institut fortlaufend über die wesentlichen rechtlichen Regelungen und Vorgaben informiert zu halten und diese aufsichtskonform umzusetzen.

Begriff Rechtsmonitoring

Der Begriff Monitoring wird allgemein als Überwachung von Vorgängen verstanden bzw. als systematische Erfassung, Messung oder Beobachtung eines Vorgangs mittels (technischer) Hilfsmittel oder anderer Beobachtungssysteme bzw. als (Dauer-)Beobachtung (eines bestimmten Systems).

Daraus folgernd sind die Kriterien eines Monitorings:

- fortlaufend,
- systematisch/planvoll,
- erfassend/dokumentierend,
- mittels eines Hilfsmittels.

Als zu monitorende Rechtsgebiete sind die Gesetzgebung, die Rechtsprechung und Aufsichtspraxis in Form von Aufsichtsmitteilungen, Merkblättern etc. einschließlich der Rundschreiben und Mitteilungen der Verbände zu nennen. Da die Regelungen und Vorgaben für Banken nicht allein auf nationalem Recht und dessen Umsetzung fußen, sondern in einem europäischen Kontext stehen, sind zumindest auch die wesentlichen Regelungen und Vorgaben auf europäischer Ebene zu berücksichtigen.

Als guter Anhaltspunkt für die zu monitorenden Themen dient im genossenschaftlichen Bereich die Musterbestandsaufnahme des BVR. Zu berücksichtigen ist jedoch, dass aufgrund des Geschäftsmodells darüberhinausgehende Normen zu beachten sind.

Die Quellen für Rechtsmonitoring-Einträge sind ganz unterschiedlich. So gibt es beispielsweise öffentlich zugängliche Quellen der Gerichte, der Bundesbank und BaFin, des Bundestages und der Bundesregierung, aber auch kostenpflichtige Datenbanken und geschlossene Informationskreise, z. B. Newsletter aus Arbeitsgemeinschaften, Berufsverbänden oder der Verbände.

Relevanz

Allerdings besteht die Besonderheit, dass die Rechtsgebiete für das jeweilige Institut relevant sein müssen. Relevanz bedeutet, dass die jeweiligen Rechtsmonitoring-Einträge zum Institut „passen“ bzw. für das Institut „einschlägig“ sein müssen, um die Institute gezielt mit den Informationen zu versorgen, die für sie notwendig und wichtig sind. Beispiel: Bei Vorgaben zur Einlagensicherung ist die Relevanz für alle Institute gegeben, da alle Institute mindestens der gesetzlichen Einlagensicherung angehören.

mehr als **4.388** Regelungen

mehr als **1.100.000** Gerichtsverfahren

1 Rechtsmonitoring

Ganz anders sieht es aber schon bei WpHG- oder verbraucherrechtlichen Rechtsgebieten aus. So gibt es Institute, die abgesehen vom Depot A, kein Wertpapiergeschäft betreiben. Für ein solches Institut sind BaFin-Vorgaben zu Fristen anlässlich einer Depotübertragung nicht einschlägig, sodass das Thema mangels Relevanz nicht in das Rechtsmonitoring für dieses Institut aufgenommen werden muss.

Augenscheinlich nicht relevante Neuerungen oder Änderungen können sich bei näherer Betrachtung jedoch als für das Institut einschlägig herausstellen. Eine sorgfältige Prüfung auch auf den ersten Blick nicht relevanter Themen ist daher zu empfehlen.

So gibt es Institute, die keine Verbraucher als Kunden haben. Bei solchen Instituten erscheint es auf den ersten Blick falsch, Rechtsmonitoring-Einträge zu erstellen, die sich auf Verbraucher-Themen beziehen.

Dass dies nicht unbedingt richtig sein muss, zeigt das Bundesgerichtshof-Urteil vom April 2021 zum AGB-Änderungsmechanismus. Das Urteil betrifft vordergründig das Verhältnis zwischen Bank und Verbraucher als Kunde, da der Bundesverband der Verbraucherzentralen und Verbraucherverbände gegen die AGB-Regelung geklagt hatte. Der BVR empfiehlt jedoch, die Rechtsprechung des Bundesgerichtshofs auch auf Nicht-Verbraucher anzuwenden, sodass die Rechtsprechung auch in einem Rechtsmonitoring Berücksichtigung finden sollte, selbst wenn die Bank keine Verbraucher als Kunden hat.

Mit der Entscheidung zur Relevanz eines Rechtsmonitoring-Eintrages ist also eine wichtige Weichenstellung verbunden, welcher Rechtsmonitoring-Eintrag in der Bank vorhanden ist und bearbeitet werden muss.

Wesentlichkeit

Neben der Relevanz gibt es noch das Kriterium der (Un-)Wesentlichkeit. Nicht alle Themen aus der Musterbestandsaufnahme bzw. den zu monitorenden Rechtsgebieten sind aus Compliance-Sicht wesentlich.

Dies kann unterschiedliche Gründe haben. So kann es sich um nicht-branchenspezifisches Recht handeln, z. B. Arbeits- und Sozialrecht oder Steuer- und Bilanzrecht, das nicht zwingend von der Compliance-Funktion überwacht werden muss, da hier ein Compliance-Risiko per se geringer ist.

Andererseits kommen aber auch Themen in Betracht, bei denen es bereits spezialisiertes Fachwissen im Haus gibt, z. B. Vorgaben zum Risikocontrolling. Hier ist es aus Compliance-Sicht ggf. möglich, eigene Aktivitäten teilweise zurückzustellen oder im Wesentlichen darauf zu verzichten. Dies bedeutet aber nicht, dass das Thema im Rechtsmonitoring nicht aufgenommen werden sollte, sondern nur, dass es unwesentlich ist; gleichwohl muss darüber gemonitort werden.

In diesem Zusammenhang stellt sich auch immer wieder die Frage, ob relevante Urteile von Amts- und Landgerichten aufgenommen werden sollen.

Man könnte argumentieren, Entscheidungen dieser Gerichte seien nicht von Bedeutung, da der Streitwert bei Amtsgerichten maximal 5.000 EUR beträgt und im Gegensatz zur Rechtsprechung der Oberlandesgerichte oder des Bundesgerichtshofes ihre Entscheidungen eher geringere Auswirkungen haben. Gleichwohl greift diese Argumentation zu kurz, da die Amtsgerichte neben den Landgerichten die Eingangskanäle für Klagen – und somit für Streitigkeiten zwischen Kunde und Bank – sind >

AUTOR UND ANSPRECHPARTNER

Jörg Scharditzky
Abteilungsleiter
MaRisk-Compliance
E-Mail: joerg.scharditzky@dz-cp.de

und Oberlandesgerichte nur für Musterverfahren nach dem Kapitalanleger-Musterverfahrensgesetz als erstinstanzliche Gerichte zuständig sind.

So ging beispielsweise bei dem oben genannten Bundesgerichtshof-Urteil zum AGB-Änderungsmechanimus der Instanzenzug vom Landgericht Köln über das Oberlandesgericht Köln hin zum Bundesgerichtshof. Berücksichtigt man auch Entscheidungen von Gerichten unterhalb des Bundesgerichtshofes, so erhält man zumindest ein gutes Indiz dafür, welche Rechtsprobleme aktuell bestehen und beim Bundesgerichtshof anhängig werden können.

Dokumentation und Umsetzung

Zur revisionssicheren Dokumentation kann beispielsweise eine Excel-Datei in einer Notes-Datenbank gespeichert, eine Datenbank oder ein Tool genutzt werden. Den Bedienungskomfort können Filtermöglichkeiten erhöhen. Verantwortunglickeiten, also welche Funktion oder Person für die Bearbeitung zuständig ist, und Priorität sollten klar erkennbar sein. Bei Prioritäten lässt sich z. B. gut mit der Ampeltechnik arbeiten.

Ein Rechtsmonitoring ist nur so gut, wie es von den Bearbeitern akzeptiert wird und in der täglichen Anwendung nutzbar ist. Dazu gehört, dass die Inhalte umgesetzt werden. Dies bedeutet, dass der in der Bank festgelegte Verantwortliche sich mit dem Inhalt beschäftigt, ihn umsetzt und dies revisionssicher dokumentiert. Für eine bessere Nachvollziehbarkeit sollte man sich nicht darauf beschränken, die Umsetzung zu bestätigen, sondern es sollten auch konkrete und nachvollziehbare Angaben dazu gemacht werden, wie die Umsetzung erfolgt ist. Idealerweise kann die erledigte Umsetzung des Handlungseintrages durch ein Dokument, einen Link oder einen beschreibenden Text etc. dokumentiert und nachvollzogen werden. Damit fällt es dann auch Dritten, z. B. der Internen Revision oder der externen Prüfung, leicht, die in der Bank erfolgte Umsetzung nachzuvollziehen.

Anbindung an Risikoanalyse

Je nach Compliance Management System erfolgt eine automatisierte Berücksichtigung des Rechtsmonitorings in der Risikoanalyse. Die Abarbeitung bzw. Reduzierung festgestellter Risiken kann beispielsweise durch umgesetzte Rechtsmonitoring-Einträge minimiert und dokumentiert werden. Durch das Zusammenspiel von Risikoanalyse und Rechtsmonitoring kann der Schutz des Institutes vor (Compliance-)Risiken effektiv gesteigert werden. Zudem wird der Compliance-Beauftragte entlastet.

Fazit

Den Überblick über die vielen Rechtsnormen und Vorgaben zu behalten, ist ein sehr schwieriges Unterfangen. Erschwert wird dies weiter durch die stetig wachsenden regulatorischen Anforderungen. Ohne Unterstützung ist dies inzwischen kaum noch zu bewerkstelligen.

Wir haben mit unserem bewährten Rechtsmonitoring, das wir im Rahmen der Auslagerungen und auch als separat buchbare Einzelleistung anbieten, bereits mehrjährige Erfahrungen sammeln können. Um Ihnen die Arbeit weiter zu vereinfachen und den Benutzerkomfort zu erhöhen, stellen wir Ihnen das Produkt Rechtsmonitoring kompakt auch als webbasiertes Tool mit Workflows zur Verfügung: Eskalationen, automatische Zuordnung von Zuständigkeiten und viele weitere Funktionen helfen Ihnen, den Blick auf das Wesentliche zu richten und revisionssicher zu dokumentieren. ▬

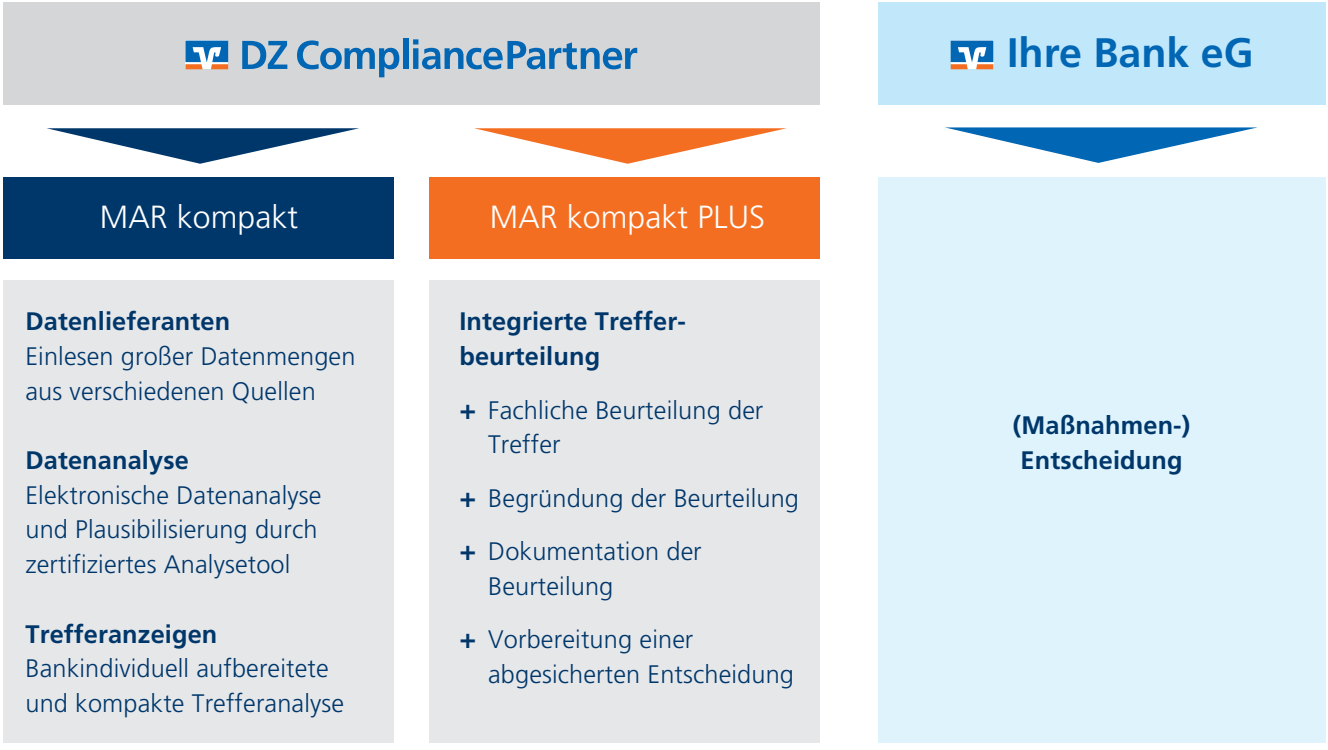
WpHG-Compliance

Umsetzung Marktmiss-brauchsverordnung

Die Anzahl der Wertpapierdepots in Deutschland hat sich – vor allem aufgrund des Niedrigzinsumfelds seit 2017 – um fast sechs Millionen Depots auf rund 28,1 Millionen Depots in 2021 erhöht. Das Deutsche Aktieninstitut verzeichnete im „Corona-Jahr" 2020 einen Anstieg bei den unter 30-jährigen Anlegern um fast 600.000. Trotz aktuell steigender Zinsen ist davon auszugehen, dass insbesondere die sogenannten „Millenials" und „Generation Z" ihr Engagement an der Börse weiter ausbauen. Der sprunghafte Anstieg der Anzahl der Depots und der damit einhergehende anwachsende Überwachungsumfang gemäß der Marktmissbrauchsverordnung (engl. Market Abuse Regulation/MAR) stellen die Institute vor große Herausforderungen.

Die BaFin stellt klar: „Betreiber von Märkten, Wertpapierfirmen, die einen Handelsplatz betreiben, und Personen, die gewerbsmäßig Geschäfte vermitteln oder ausführen, sind ab 2. Juli 2016 gemäß Artikel 16 Absatz 1 und 2 der Marktmissbrauchsverordnung (MAR) verpflichtet, Aufträge und Geschäfte, die Insidergeschäfte, Marktmanipulationen oder der Versuch hierzu sein könnten, unverzüglich der BaFin zu melden." (https://www.bafin.de/DE/DieBaFin/Service/MVPportal/Verdacht_MAR/verdacht_mar_node.html)

ABB. 1 MIT MAR KOMPAKT PLUS LAGERN SIE DIE TREFFERBEURTEILUNG AUS



Mögliche Arbeitserleichterungen

Um die anspruchsvolle Überwachung auf effiziente Weise in den Griff zu bekommen und gleichzeitig die Personalressourcen für das Kerngeschäft freizuhalten, bietet sich ein Zurückgreifen auf externe Unterstützung an. Möglichkeiten gibt es dabei am Markt einige.

So können beispielsweise Tools zur Trefferbearbeitung eingesetzt werden. Mit einer richtigen Parametrisierung können diese helfen, den Blick auf die relevanten Treffer zu richten. Die Parametrisierung ist jedoch mit einem nicht unerheblichen Aufwand verbunden.

Eine erweiterte Möglichkeit ist der Bezug täglich erstellter Listen verdächtiger Geschäfte, wie sie beispielsweise auch von uns mit MAR kompakt angeboten werden. Diese Trefferliste dient der systematischen Überwachung der Kunden-, Mitarbeiter- und Bankgeschäfte in Finanzinstrumenten zur Erkennung potenziell marktmanipulativer Handlungen.

Schlussendlich besteht die Möglichkeit, die Überwachung gemäß Marktmissbrauchsverordnung auszulagern. Das impliziert dann auch die Bewertung der Trefferübersichten, wie sie beispielsweise mit MAR kompakt PLUS angeboten wird.

MAR kompakt PLUS

Bei dieser (Teil-)Auslagerung wird die fachliche Beurteilung der Marktmissbrauchstreffer und Mitarbeitergeschäfte von einem qualifizierten Team übernommen: Unser Team wird fortlaufend auf dem aktuellen Stand der rechtlichen Anforderungen gehalten und verfügt über einen umfangreichen Erfahrungsschatz.

Die Trefferbearbeitung erfolgt dabei noch am gleichen Tage und wird revisionssicher dokumentiert. Vertretungsregelungen in der Bank entfallen ebenso wie die Notwendigkeit zur Aufrechterhaltung der Sachkunde gemäß Marktmissbrauchsverordnung.

Um eine gezielte Insiderüberwachung zu ermöglichen, kommen verschiedene Instrumente zum Einsatz. Die Ergebnisse aus Befragungen der Mitarbeiter zu potenziellen Insidersituationen können über eine Watchlist und eine Liste besonderer Marktteilnehmer einer gezielten Überwachung zugeführt werden. Diese Listen können auch Underlyings überwachen und sind an eine dynamische handelsvolumenabhängige Großorderberechnung geknüpft. Neben den Überwachungswerkzeugen von MAR kompakt müssen keine weiteren Überwachungstools genutzt werden.

Besteht ein Verdacht auf Marktmissbrauch bzw. sollte es zu Handlungsbedarf durch Ihr Haus kommen, setzen wir uns umgehend mit Ihnen in Verbindung. Im Falle einer Anzeige bereiten wir das Meldeformular zum Upload im BaFin-Portal vor. Darüber hinaus stehen wir Ihnen beim Umgang mit Grenzfällen beratend zur Seite. Die Bank erhält quartalsweise eine Zusammenfassung der geprüften Geschäfte, bei der auch die getätigten Verdachtsmeldungen und Verstöße gegen Mitarbeiterleitsätze abgebildet werden.

Alle Systematiken und Kriterien sind transparent und nachvollziehbar und entsprechen damit den Anforderungen einer Teilauslagerung. Die Bank erhält für diese Teilauslagerung eine nach IDW-Standard zertifizierte Leistung (IDW PS 951 Typ II), die Technik ist nach IDW PS 880 zertifiziert.

Fazit

Es ist davon auszugehen, dass die Anzahl an Wertpapiertransaktionen auch in Zukunft weiter steigen wird und somit weitere Ressourcen zur Marktmissbrauchsverhinderung in den Instituten binden wird. Es ist von daher zu empfehlen, dass sich die Institute bereits heute mit der weiteren Entwicklung befassen, um ausreichend Personalressourcen zur Bewältigung der Aufgaben vorzuhalten. Alternativ sollte der Einsatz von Unterstützungsprodukten, wie beispielsweise der Trefferbearbeitung, geprüft werden. ▬

AUTOREN UND ANSPRECHPARTNER

Mona Baitinger
Abteilungsleiterin
Compliance-Analysten
E-Mail: mona.baitinger@dz-cp.de

Jenny Engemann
Analystin WpHG-Compliance
E-Mail: jenny.engemann@dz-cp.de

Interne Revision

Regelmäßig berichten wir an dieser Stelle über die Interne Revision der DZ CompliancePartner GmbH. Wir möchten Ihnen damit einen Überblick über die Qualität der unterschiedlichen Auslagerungsdienstleistungen geben und Sie in Ihrem Auslagerungscontrolling unterstützen. Die durchgeführte Revisionstätigkeit der DZ CompliancePartner GmbH genügt den Anforderungen gemäß MaRisk AT 4.4.3 und BT 2.

Seit der letzten Berichterstattung in der Point of Compliance (3/2021, S. 23) wurden entsprechend der Jahresprüfungsplanung 2021 zwei weitere Prüfungen abgeschlossen. Hierbei handelt es sich um „Unternehmenssteuerung – Rechnungswesen & Controlling“ und „IT & Projekte – Allgemeine Betriebsorganisation & Dienstleistersteuerung“. Da diese interne Bereiche betreffen, werden die Prüfungsberichte zu den beiden Geschäftsbereichen lediglich intern veröffentlicht. Unter Berücksichtigung einer Prüfungsanpassung wurde der Prüfungsplan 2021 vollumfänglich erfüllt. Die Prüfungsanpassung betrifft die Prüfung „IT & Projekte - Projektorganisation und -abwicklung“, die auf das laufende Jahr verschoben wurde, da die Projekte erst am Ende des letzten Jahres planmäßig abgeschlossen wurden.

Aus der Jahresprüfungsplanung 2022 wurden die Prüfungen des Bereichs „Hinweisgebersystem“ und der Geschäftsbereiche „MaRisk-Compliance“ und „WpHG-Compliance“ abgeschlossen und diese dienstleistungsbezogenen Berichte der Mandantschaft mit der entsprechenden Auslagerung zur Verfügung gestellt.

Darüber hinaus wurde ein Bericht zum Prüffeld „IT & Projekte – Projektorganisation und -abwicklung“ abgeschlossen und, da nicht dienstleistungsbezogen, intern veröffentlicht.

Die Quartalsberichte zum vierten Quartal 2021 und zum ersten und zweiten Quartal 2022 der Internen Revision wurden fristgerecht erstellt und unseren Kunden zur Verfügung gestellt. Ebenso wurde der Jahresbericht 2021 der Internen Revision fristgerecht an die Kunden, die 2021 zu unserem Kundenstamm zählten, versandt.

Darüber hinaus wurden turnusgemäß ein Follow-up-Quartalsbericht für das vierte Quartal 2021 und für das erste und zweite Quartal 2022 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen bzw. Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

Als weiterer Informationsaustausch finden zwischen dem Sprecher der Geschäftsführung der DZ CompliancePartner GmbH und der Internen Revision regelmäßige Jours fixes statt.

Die externe Prüfung der Geschäftsbereiche Datenschutz, Geldwäsche- und Betrugsprävention, Informationssicherheit, MaRisk-Compliance und WpHG-Compliance nach IDW PS 951 (Typ 2) wurde von der Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft vorgenommen. Für alle Bereiche wurde jeweils ein Testat ohne wesentliche Einschränkung erteilt. Die Endfassungen der Berichte zur externen Prüfung wurden an die Kunden der jeweiligen Dienstleistung versandt.

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 erfolgte ebenfalls durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft. Es wurde die Ordnungsmäßigkeit testiert und auch hier wurde der Prüfungsbericht an die Mandantschaft versandt.

Wie bereits seit 2008 wurde uns erneut eine TÜV-Zertifizierung zum Notfall-Management vom TÜV Saarland erteilt, der damit die Konformität des Notfallkonzepts nach MaRisk AT 7.3 testiert. ▬

Ansprechpartner: ***Lars Schinnerling,***
Bereichsleiter Interne Revision, E-Mail: lars.schinnerling@dz-cp.de

Wirtschaftliche Lage

Das Ergebnis der DZ CompliancePartner GmbH liegt Ende Juli – bereinigt um den Verkaufserlös der Sparte IT-Audit (IT-Revision) – über Plan.

Die Erlöse lagen kumuliert 58 TEUR über Plan (Plan: 9.779 TEUR), der Aufwand hingegen 69 TEUR unter Plan (Plan: -9.068 TEUR). Hieraus ergibt sich kumuliert eine Planüberschreitung von +127 TEUR.

Die DZ CompliancePartner GmbH geht davon aus, dass sich die Erlösüberschreitung in den kommenden Monaten nicht fortsetzen wird, sondern sich rückläufig entwickeln wird. ▬

Ansprechpartner: ***Jens Saenger,***
Sprecher der Geschäftsführung, E-Mail: jens.saenger@dz-cp.de