Cyber Security

Booklet

STADLER VÖLKEL
RECHTSANWÄLTE · ATTORNEYS AT LAW

Hi there, welcome to #sv.law

Intro

Cyber-Sicherheit spielt in der heutigen Zeit eine immanente Rolle. Dies einerseits, weil sich Cyber-Vorfälle (etwa Cyber-Angriffe) häufen und vermehrt zu Schäden führen; andererseits, weil rechtliche Verpflichtungen in diesem Zusammenhang sowie an die Cyber-Sicherheit angelegte Maßstäbe kontinuierlich zunehmen.

Die Europäische Union sowie andere Akteure haben die Bedeutung von Cyber-Sicherheit erkannt und zielführende Maßnahmen bereits normativ festgelegt oder zumindest in Form von Soft-Law als Empfehlungen herausgegeben. Die Vielzahl derartiger Vorgaben führt zwar zu einem Dschungel von Regularien, doch ist dieser oftmals dem technologischen Fortschritt mit stets neuen Herausforderungen geschuldet. Mit zunehmendem Digitalisierungsgrad nimmt auch das Cyber-Risiko zu. Der europäische und nationale Gesetzgeber haben daher kaum eine andere Wahl als zu reagieren.

Dieses Booklet soll die zentralen Aspekte der Cyber-Sicherheit aus rechtlicher Perspektive beleuchten und auf verständliche Weise vermitteln. Für eine Behandlung von Detailfragen oder eine rechtliche Beratung in Zusammenhang mit konkreten Projekten stehen die Cyber-Law-Experten von STADLER VÖLKEL Rechtsanwälte gerne zur Verfügung.

Cyber-Security-Recht

Der Begriff "Cyber-Security-Recht" lässt sich zwar nicht einheitlich definieren. Für dieses Booklet werden darunter jedoch jene Rechtsnormen und Leitlinien verstanden, die im Kontext von Cyber-Sicherheit von besonderer Relevanz sind.

Europarechtliche Einflüsse spielen hierbei eine besonders große Rolle. Allen voran sieht bereits die geltende DSGVO der Europäischen Union einen gültigen Mindeststandard an Cyber-Sicherheit vor. Weitere Verpflichtungen ergeben sich insbesondere auch aus der nationalen Umsetzung der Netz- und Informationssystemsicherheits-Richtlinie, dem "NISG", in Verbindung mit der darauf aufbauenden NIS-Verordnung.

Die nationale Umsetzung der diesbezüglichen Nachfolge-Richtlinie "NIS2" ist seitens Österreich derzeit zwar noch nicht erfolgt, wird aber den Anwendungsbereich für vorgeschriebene Cyber-Sicherheit signifikant erweitern.

Darüber hinaus werden sich in Kürze wirksame Vorgaben an die Cyber-Sicherheit in der ebenfalls auf europäischer Ebene erlassenen Verordnung (EU) 2022/2554, besser bekannt als Digital Operation Resilience Act ("DORA"), finden. Ergänzend dazu wird derzeit über einen Vorschlag des Cyber Resilience Acts ("CRA") verhandelt.

Im Lichte von Cyber-Sicherheit sei auch die Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte ("MiCAR") erwähnt, die auch für Krypto-Börsen ein gewisses Maß an Cyber-Sicherheit vorschreiben wird.

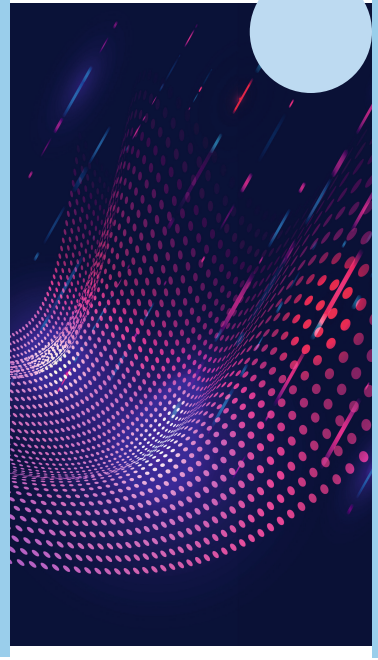
Hinsichtlich Soft-Law existieren unter anderem für die Bank- und Finanzwirtschaft relevante Leitlinien der Europäischen Bankenaufsicht ("EBA").

Wenngleich es aufgrund verschiedenster Rechtsakte mit teilweisen Überlappungsbereichen zu einem gewissen Wildwuchs gesetzlicher Bestimmungen kommt, so ist die Cyber-Sicherheitsstrategie des Gesetzgebers insgesamt jedenfalls begrüßenswert, um mit der Digitalisierung auch aus Sicherheitsaspekten mithalten zu können.

Datenschutz schreibt auch Cyber Security vor!

Ein allgemeines Verständnis des Begriffs "Datenschutz" lässt sich rasch gewinnen: In einem weiten Sinn kann darunter alles er- und aufgefasst werden, was sich – aus welchem Grund auch immer – mit dem Schutz von Informationen durch bestimmte Vorkehrungen beschäftigt. Im Detail wird die Begrifflichkeit allerdings weder einheitlich definiert noch verstanden.

Die dafür derzeit maßgebliche Rechtsnorm ist die Datenschutz-Grundverordnung ("DSGVO") der Europäischen Union. Vielfach wird jedoch außer Acht gelassen, dass diese neben datenschutzrechtlichen Kernverpflichtungen und -rechten auch ein Mindestmaß an Cyber-Sicherheitsmaßnahmen vorschreibt.



Cyber-Sicherheitsvorgaben in der DSGVO

So findet sich etwa in Artikel 32 Absatz 1 der DSGVO der Verweis auf die Sicherheit der Verarbeitung "[u]nter Berücksichtigung des Stands der Technik" sowie die Verpflichtung "geeignete technische und organisatorische Maßnahmen [zu treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten".

Verstößt der datenschutzrechtlich Verantwortliche oder der Auftragsverarbeiter gegen diese Vorgaben, drohen Bußgelder sowie Schadenersatzansprüche datenschutzrechtlich Betroffener, denen Schäden entstanden sind. Neben diesem "unschönen" rechtlichen Nachspiel kann die fehlende oder mangelnde Cyber-Sicherheit jedoch auch das Risiko erhöhen, Opfer eines Cyber-Vorfalls zu werden – Cyber-Sicherheit sollte deshalb bereits im Eigeninteresse gelebt werden.

Darüber hinaus sollte das Bewusstsein bestehen, dass der Eintritt eines Cyber-Vorfalls auch datenschutzrechtliche Meldeverpflichtungen auslösen kann.

Cyber-Vorfall?

Meldung von Datenschutzverletzungen!

Ozzy Osbourne sagte einst: "Von allem, was ich verloren habe, vermisse ich meinen Verstand am meisten!"

Auch personenbezogene Daten haben es an sich, teilweise verloren zu gehen – sei es ungewollt, bspw. durch Sicherheitslücken in datenverarbeitenden Systemen, oder im Zuge der Nachlässigkeit eines Verantwortlichen bewusst in Kauf genommen. Zwar sind Daten zum Glück nicht gleich der Verstand – aber auch sie werden von den Betroffenen oft schmerzhaft vermisst. Dabei könnte deren Verlust gerade mit vorausschauendem Scharfsinn allzu oft verhindert werden.

Was muss ich tun, wenn mir Daten abhandenkommen oder sich ein Cyber-Vorfall ereignet?

Sollte es zu einer Verletzung des Schutzes personenbezogener Daten kommen (sog. "Data Breach"), ist schnelles und entschlossenes Handeln gefragt!

Zunächst muss in den allermeisten Fällen innerhalb von 72 Stunden ab Kenntnis der Verletzung eine Meldung an die zuständige Aufsichtsbehörde vorgenommen werden. In ihr müssen bestimmte Mindestangaben über den Vorfall enthalten sein; so etwa die Art der Verletzung, ihre wahrscheinlichen Folgen und die zu ihrer Beseitigung angedachten Maßnahmen.

Die betroffenen Personen sind von der Verletzung hingegen grundsätzlich nur dann zu unterrichten, wenn daraus ein hohes Risiko für ihre Rechte und Freiheiten resultiert.

Zuckerbrot und Peitsche:

Sanktionen und Rechtsdurchsetzung

Obgleich die DSGVO die Konformität mit datenschutzrechtlichen Bestimmungen, damit etwa auch Cyber-Sicherheitsvorgaben gemäß Artikel 32, fröhlich der Selbstverantwortung der Rechtsunterworfenen überlässt, straft sie aufgedeckte Verfehlungen umso hemmungsloser ab.
Das betraf vor allem die "üblichen Verdächtigen" wie Facebook, Amazon, Google & Co., bei welchen datenschutzrechtliche Überlegungen lange Zeit keinen allzu hohen Stellenwert eingenommen haben – aber auch kleine und mittelgroße Unternehmen bekamen den Zorn der Aufsichtsbehörden schon zu spüren. Der Rahmen der verhängten Sanktionen reichte dabei von bloßen Verwarnungen bis zu Strafen im Bereich mehrerer hundert Millionen Euro!
Trotz der für den einfachen Mann astronomischen Summen bleibt allerdings dennoch zu bedenken: Auch die höchsten der bisherigen Bußgelder fallen speziell für die abgestraften Großkonzerne aufgrund ihrer enormen wirtschaftlichen Kapazitäten nicht wirklich ins Gewicht.

Wie kommt es zu derartigen Summen?

Die Höhe der Bußgelder wird von Aufsichtsbehörden – mit einem weiten Ermessenspielraum – festgelegt (bis zu EUR 20 Millionen oder 4 % des weltweiten Jahresumsatzes; für Verstöße gegen Cyber-Sicherheitsvorgaben bis zu EUR 10 Millionen oder 2 % des weltweiten Jahresumsatzes). Außerdem stehen diesen Behörden zusätzliche Werkzeuge zur Reaktion auf Verstöße gegen das Datenschutzrecht, wie etwa die Untersagung von weiteren Verarbeitungen, zur Verfügung. Probleme für Verantwortliche können sich dabei schon dadurch ergeben, dass sie ihr ggf. datenschutzkonformes Verhalten nicht nachzuweisen vermögen und damit die allgemeine Rechenschaftspflicht der DSGVO verletzen.

Aber auch betroffene Personen müssen bei einer Verletzung datenschutzrechtlicher Vorschriften nicht tatenlos zusehen: Zum einen können sie ggf. auf ihr Beschwerderecht bei einer Aufsichtsbehörde zurückgreifen, sollten datenschutzrechtliche Pflichten nicht eingehalten werden, oder sie machen eine Verletzung ihrer subjektiven Rechte als betroffene Personen vor den ordentlichen Gerichten geltend. Auch können sie unter gewissen Voraussetzungen Schadenersatz verlangen.

Netz- und Informationssysteme

Cyber-Sicherheitsmaßnahmen sind für bestimmte vom Gesetzgeber explizit angeführte Bereiche von ganz besonderer Bedeutung. Deshalb sieht etwa das Netz- und Informationssystemsicherheitsgesetz ("NISG"), als nationales Umsetzungsgesetz der entsprechenden EU-Richtlinie, Cyber-Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie für Einrichtungen der öffentlichen Verwaltung vor.

So haben etwa gem. § 17 Abs 1 NISG "Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein."

Ähnliches gilt gem. § 21 Abs 1 NISG für "Anbieter digitaler Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des digitalen Dienstes nutzen". Solcherart erfasste Anbieter haben "geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen".

Selbst Einrichtungen der öffentlichen Verwaltung bleiben diesmal nicht vor Sicherheitsverpflichtungen verschont, wenngleich sich unmittelbare Pflichten vorwiegend an Bundeseinrichtungen richten.

Neben der Durchführungsverordnung (EU) 2018/151 der Europäischen Kommission werden entsprechende Vorgaben durch die Netz- und Informationssystemsicherheitsverordnung ("NISV"), in deren Anhang eine umfangreiche Auflistung der einzuhaltenden Maßnahmen zu finden ist, konkretisiert. Auch diese gilt es daher zu berücksichtigen.

Die NISV

Netz- und Informationssicherheitsverordnung

Die NISV liefert mehr Details zu den erforderlichen Sicherheitsmaßnahmen und gibt Einblicke in die Vorstellung des Gesetzgebers.

Sie umfasst unter anderem die folgenden Aspekte:

- Governance & Risikomanagement
- Umgang mit Dienstleistern, Lieferanten & Dritten
- Identitäts- & Zugriffsmanagement
- Systemwartung & Betrieb
- Physische Sicherheit
- Erkennung von Vorfällen
- Bewältigung von Vorfällen

Folgen von Verstößen

gegen Cyber-Sicherheitsmaßnahmen im NISG

Wird gegen gesetzliche Verpflichtungen verstoßen, so drohen insbesondere Verwaltungsstrafen. Bei Verstößen können Geldstrafen bis zu EUR 50.000 bzw. im Wiederholungsfall bis zu EUR 100.000 betragen. Darüber hinaus sind auch Schadenersatzansprüche Geschädigter denkbar.

Ausblick: NIS2-Richtlinie

Netz- und Informationssystemsicherheitsrichtlinie #2

Mit der Richtlinie (EU) 2022/2555 ("NIS2-RL") gibt es nunmehr eine Nachfolgeregelung der derzeit im nationalen NISG umgesetzten NIS-RL. Die NIS2-RL ist von den Mitgliedstaaten der Europäischen Union bis zum 17. Oktober 2024 in nationales Recht umzusetzen. Die diesbezüglichen Regelungen – inklusive Vorschriften zur Cyber-Sicherheit – sind ab dem 18. Oktober 2024 anzuwenden und zu vollziehen. Im Vergleich zur Vorgängerregelung wird der Kreis der zur Cyber-Sicherheit verpflichteten Unternehmen mit der NIS2-RL wesentlich vergrößert. Eine Vielzahl bisher nicht betroffener Unternehmen müssen sich nun von Gesetz wegen mit Cyber-Sicherheit auseinandersetzen und diese sicherstellen. So ist etwa nunmehr auch eine Einrichtung in einem Mitgliedstaat erfasst, bei der es sich – unabhängig von der Größe – "um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist" und etwa dem Sektor Bankwesen zuzuordnen oder als Anbieter digitaler Dienste zu qualifizieren ist. Darüber hinaus ist nun etwa auch ein privates Lebensmittelunternehmen, welches in der Europäischen Union tätig und zumindest als mittleres Unternehmen zu qualifizieren ist, von der NIS2-RL betroffen. Verstöße gegen die in der NIS2-RL enthaltenen Verpflichtungen können mit "Geldbußen mit einem Höchstbetrag von mindestens 10 000 000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmen[s]" geahndet werden, je nachdem welcher Betrag höher ist. Hier besteht nationaler Umsetzungsspielraum.

Digital Operation Resilience Act

(DORA)

Der Digital Operational Resilience Act ("DORA") wurde am 27. Dezember 2022 als Verordnung (EU) 2022/2554 im Amtsblatt der Europäischen Union veröffentlicht und normiert Verpflichtungen an die Normunterworfenen. Anders als bei der NIS2-RL bedarf es keiner nationalen Umsetzung, sodass die Verordnung in der Europäischen Union vollharmonisiert und damit einheitlich für alle Mitgliedstaaten gilt.

Im Zentrum von DORA steht ein Rechtsrahmen für die digitale Betriebsstabilität. Angesichts zunehmender Cyber-Kriminalität, Cyberangriffe und Datenmissbrauchsfälle sollen Finanzunternehmen wie Banken, Versicherungsunternehmen, Zahlungsdienstleister und deren IKT-Dienstleister ihre Cyber-Sicherheit stärken und deren Stabilität im Falle von IKT-Bedrohungen gewährleisten. Der europäische Finanzsektor soll dadurch seine Stabilität auch im Falle schwerwiegender Störungen aufrechterhalten können und die Risiken vermindern, die mit der Digitalisierung einhergehen.

Digital Operation Resilience Act

(DORA)

Die Ziele von DORA sollen durch digitale Sicherheits- und Berichterstattungspflichten für die betroffenen Finanzunternehmen erreicht werden. Konkret bestimmt DORA für alle Finanzunternehmen:

- die Einrichtung tauglicher und stabiler IKT-Systeme;
- die Implementierung von IKT-Risikomanagementrahmen einschließlich regelmäßiger Überprüfungen der IKT-Systeme durch risikobasierte Testungen;
- Melde- und Berichterstattungspflichten über schwerwiegende IKT-Vorfälle; sowie
- den Informationsaustausch über IKT-Risiken zwischen den Finanzunternehmen.

Außerdem soll das gesamte IKT-Lieferantennetzwerk in die IKT-Risikobewertung integriert werden. Dafür fordert DORA ein IKT-Drittparteirisikomanagement. Finanzunternehmen haben IKT-Dienstleister daher bereits vor Auftragserteilung mittels Risikoanalyse zu überprüfen.

Das IKT-Risikomanagement orientiert sich dabei an technischen Regulierungsstandards (RTS) und Leitlinien. Darüber hinaus ist bis zur Geltung von DORA eine österreichische Begleitgesetzgebung zu erwarten, da DORA den Mitgliedstaaten zahlreiche Wahlrechte einräumt.

DORA sorgt für harmonisierte IT-Sicherheitsstandards auf EU-Ebene, was den europäischen Finanzsektor attraktiver und beständiger machen kann. Durch den weiten Anwendungsbereich besteht aber für Finanzunternehmen rascher Handlungsbedarf, da die Anforderungen der DORA bereits bis zum 17. Jänner 2025 umgesetzt werden müssen.

Cyber-Security

für die Bank- und Finanzwirtschaft & für Krypto-Anbieter

Für den ohnehin schon streng regulierten Bank- und Finanzsektor kommen hinsichtlich Cyber-Sicherheit zusätzlich zu den bereits genannten Regularien auch Leitlinien der Europäischen Bankenaufsicht ("EBA") zum Tragen. Teilweise betreffen diese sogar die anzuwendende Vollzugspraxis nationaler Aufsichtsbehörden.

Die im Lichte der Cyber-Sicherheit besonders relevanten Leitlinien finden sich unter anderem in EBA/GL/2017/05, EBA/GL/2019/04 sowie in EBA/GL/2019/02. Der Adressatenkreis reicht von Zahlungsdienstleistern, Kreditinstituten und Wertpapierfirmen bis zu den bereits erwähnten Aufsichtsbehörden.

Darüber hinaus treffen laut derzeitigem Entwurf der Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte ("MICAR") in Zukunft auch Kryptodienstleister entsprechende Cyber-Sicherheitsregeln. Für diese ist Cyber-Sicherheit sogar Zulassungsvoraussetzung.

Leitlinien der europäischen Bankenaufsicht

Beispielhafte Vorgaben

Die Leitlinien der Europäischen Bankenaufsicht regeln etwa die folgenden Aspekte:

- Organisation & Governance
- Logische Sicherheit
- Physische Sicherheit
- IKT-Betriebssicherheit
- Sicherheitsüberwachung
- Schulung und Sensibilisierung hinsichtlich Informationssicherheit

Die Vorgaben an die Cyber-Sicherheit ähneln jenen in der NISV. Dies verwundert allerdings nicht weiter, sind doch die für Cyber-Sicherheit maßgeblichen Aspekte meist dieselben.

Ein ganz besonders großer Stellenwert kommt in diesem Zusammenhang dem Faktor Mensch zu. Die besten technologischen Sicherheitseinrichtungen nützen nicht viel, wenn es Personen gibt, die diese umgehen oder sich manipulieren bzw. instrumentalisieren lassen.

Ausblick: Cyber Resilience Act

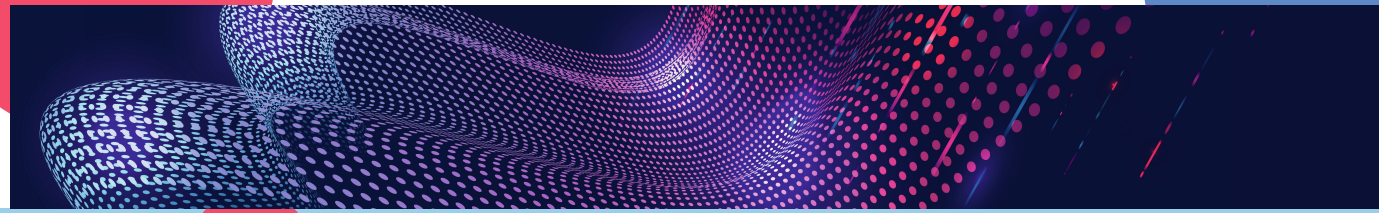
Es existiert zwar noch keine finale Version der EU-Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen ("CRA"); doch ist bereits jetzt klar, dass neue Cyber-Sicherheitsmaßnahmen auf unterschiedliche Akteure und Adressaten zukommen werden. So ist erklärtes Ziel des CRA insbesondere "Vorschriften für das Inverkehrbringen von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten", einzuführen. Diese Anforderungen sollen bereits in der Konzeptionsphase von Produkten mit digitalen Elementen relevant werden.

Die konkreten Maßnahmen, welche es einzuhalten gilt, finden sich in einer separaten Reihe von Anhängen. Deren Anhang I umfasst hierbei grundlegende Cybersicherheitsanforderungen, etwa dass Produkte mit digitalen Elementen ohne bekannter ausnutzbarer Schwachstelle ausgeliefert werden müssen. Darüber hinaus muss der von der Verordnung erfasste Hersteller eine Bewertung der Cybersicherheitsrisiken, die ein Produkt mit digitalen Elementen birgt, durchführen.

Flankiert werden die vorgesehenen Maßnahmen von Sanktionen unterschiedlichen Grades.

Derzeit befindet sich der Vorschlag für den CRA noch im europäischen Gesetzgebungsprozess und sieht eine Geltung innerhalb von 12–24 Monaten nach Inkrafttreten vor.

Haftung für das Management



Oftmals sind die für Verstöße gegen vorgeschriebene Cyber-Sicherheitsmaßnahmen vorgesehenen Straf- und Haftungsnormen direkt auf Unternehmen zugeschnitten. Denkbar sind aber freilich auch Ansprüche gegenüber natürlichen Personen, etwa aus dem Management. Hierzu kommen einerseits unmittelbare Verwaltungsstrafen, andererseits aber auch Schadenersatzansprüche infrage.

Letztere spielen insbesondere im Zusammenhang mit Regressen der juristischen Person gegenüber dem Management eine wesentliche Rolle, kommt diesem doch oftmals eine Verpflichtung zur Umsetzung spezifischer Cyber-Sicherheitsmaßnahmen zu.

Die sog. Safe-Harbor-Regelung der Business Judgement Rule, welche bei Erfüllen der ihr zugrundeliegenden Voraussetzungen zu einer Haftungsbefreiung des Managements führt, greift in diesem Zusammenhang nur dann, wenn entsprechend sorgfältig gehandelt wurde. Wurden etwa unternehmerische Entscheidungen – dies kann zum Beispiel die bewusste Entscheidung gegen bestimmte Cyber-Sicherheitsmaßnahmen sein –

nicht aufgrund angemessener Information und zum vermeintlichen Wohle der Gesellschaft getroffen, greift die Haftungsbefreiung der Business Judgement Rule nicht und es besteht ein Haftungsrisiko des Managements. Um überhaupt aufgrund angemessener Informationen handeln zu können, ist es notwendig solche einzuholen. Das wird in Bezug auf gesetzlich vorgeschriebene Cyber-Sicherheitsmaßnahmen üblicherweise die Expertise eines Juristen sowie eines Technikers erfordern.

Dementsprechend wichtig ist es, über entsprechende Sachkenntnis zu verfügen und diese zu nützen.

Verschärft wird das Thema der Haftung, insbesondere für Gesellschaften, aufgrund der Verbandsklage-Richtlinie, die Massenverfahren erleichtern soll.

Unsere Checkliste zur Verbesserung der allgemeinen Cyber-Sicherheit

Im Folgenden soll eine Hilfestellung bei der Verbesserung der Cyber-Sicherheit geliefert werden. Dies trägt nicht nur zu erhöhter Compliance, sondern auch zu einer faktischen Risikoreduktion bei.

1. Ist die Belegschaft adäquat zu Cyber-Sicherheit und Datenschutz geschult?
2. Wurden interne Compliance-Systeme etabliert?
3. Gibt es einen Datenschutzbeauftragen?
4. Werden regelmäßige (externe) Sicherheitsüberprüfungen durchgeführt?
5. Werden entsprechend identifizierte Defizite angemessen behoben?
6. Sind Perimeter-Systeme, wie etwa Firewalls, adäquat konfiguriert?
7. Besteht ausreichendes Bewusstsein bezüglich anwendbarer rechtlicher Verpflichtungen?
8. Gibt es adäquate Backup-Systeme, die auch über räumlich getrennte Speicherorte verfügen?
9. Gibt es Sicherheitseinrichtungen nach dem Stand der Technik?
10. Werden veraltete Systeme verwendet? Wenn ja, werden diese besonders geschützt?

Dein SV.LAW-Team

für den Bereich Cyber Security

Arthur Stadler

Thomas Seeber

Tamino Chochola

Christopher Drolz

Felix Bauer

STADLER VÖLKEL
RECHTSANWÄLTE · ATTORNEYS AT LAW

Grafikdesign
Mag. Stefanie Wagner

Bildnachweise
Adobe Stock

Druckhersteller
online Druck GmbH
Brown-Boveri-Straße 8
2351 Wr. Neudorf

IMPRESSUM
STADLER VÖLKEL Rechtsanwälte GmbH
Seilerstätte 24, 1010 Wien

Tel.: +43 1 997 1025
Fax: +43 1 997 1025 99

office@sv.law
www.sv.law
Booklet Cyber Security: Stand März 2023