Ausgabe 2023

reichert reichert
steuern . recht . consulting

mitdenken

Digitale Transformation

„Chancen und Herausforderungen“

Liebe Leserinnen und Leser,

Nach zwei spannenden Kanzleimagazinen zum Themenbereich „Immobilien“ und zum „Verschenken und Vererben“ im vergangenen Jahr, freuen wir uns sehr, Ihnen heute erneut ein Magazin mit vielseitigen und sicherlich für uns alle aktuellen Fokusthemen präsentieren zu dürfen.
Unser Kanzleiteam hat sich diesmal mit einem breiten Spektrum der Chancen und Herausforderungen durch „digitale Transformation“ auseinandergesetzt.
Ein Thema, das fast allen von uns beinahe täglich in der einen oder anderen Ausprägung begegnet, das unsere Geschäftsmodelle und unsere Organisation herausfordert, das uns auffordert, organisatorische Routinen zu hinterfragen und das, darüber besteht heute wohl kaum mehr Zweifel, die Arbeitswelt der Zukunft verändern und zum Teil neu erfinden wird.
Dabei erleben wir in unserer Beratungspraxis, wie vielfältig unsere Mandantschaften auf den digitalen Wandel reagieren und wie viele Chancen sich aus dem intelligenten Einsatz moderner Informationstechnologie heben lassen. Gleichzeitig dürfen wir uns — nicht zuletzt auch in der rechtlichen Beratung unserer Mandantschaften — in veränderten Situationen und in einem veränderten, digitalen Umfeld erfolgreich positionieren.
Das Team der Kanzlei reichert & reichert steht Ihnen dabei mit vielfältigen Kompetenzen und gewohnt praktischer, praxisnaher und lösungsorientierter Beratung zur Seite.
In diesem Sinne freuen Sie sich auf eine anregende und spannende Lektüre. Wir freuen uns auf Ihre Fragen und wünschen Ihnen viel Spaß beim Lesen.

Herzlichst Ihr Dr. Hansjörg Reichert

INHALT

HERAUSGEBER

reichert & reichert
steuerberater & rechtsanwaltskanzlei
Max-Porzig-Straße 1 – 78224 Singen
+49 (0) 7731 9587-0
Reichenaustraße 19a – 78467 Konstanz
+49 (0) 7531 81987-0
kanzlei@reichert-reichert.de

Redaktion
Dr. Hansjörg Reichert, Matthias Herkert,
Nils Stark, Chiara Bidmon, Eileen Binder,
Lisa-Sabrina Thum, Carina Meyer, Marie-Luis Bufler
Layout
Kieweg und Freiermuth GmbH – www.kuf.com
Fotografie
www.frank-com.de
shutterstock.com

DAS THEMA DER NÄCHSTEN AUSGABE:
Unternehmens-nachfolge

erschienen im Juni 2023

Rechtliche Besonderheiten im IT-Vertragsrecht

Der Bereich des IT-Vertragsrechts mutet unter anderem durch die Notwendigkeit der Abbildung komplexer IT-Anforderungen, vieler technischer Begrifflichkeiten und nicht zuletzt durch den Bedarf zur Regelung meist virtueller Themen oftmals exotisch an. Nachfolgend wollen wir klären, ob dies tatsächlich der Fall ist. Innerhalb dieser Betrachtung des IT-Rechts widmen wir uns zunächst den vertragsrechtlichen Grundlagen. Anschließend werden Besonderheiten in der Vertragsgestaltung sowie die Unterstützungsmöglichkeiten bei Rechtsstreitigkeiten dargestellt.

WAS IST EIN IT-VERTRAG?

Die Bezeichnung „IT-Vertrag" ist rechtstechnisch gesehen nicht korrekt, da es keinen gesonderten Vertragstyp im Bereich des IT-Rechts gibt. Vielmehr sind auch Verträge aus dem IT-Recht unter die, generell im Bürgerlichen Gesetzbuch existierenden Vertragstypen wie beispielsweise den Kauf-, Werk-, Dienst- oder Mietvertrag einzuordnen.

Die Besonderheit der Vertragsgestaltung, also die Abweichung von der Norm dieser Vertragstypen, liegt dabei im Wesentlichen im Vertragsgegenstand, welcher so breit gefächert sein kann, dass er von der Programmierung einer Individualsoftware über die Vermietung einer Standardsoftware auf Zeit bis hin zum Kauf von Hardware reichen kann.

KLÄREN SIE DEN VERTRAGSGEGENSTAND, BEVOR SIE SICH AUF DEN WEG MACHEN!

Die Einordnung des jeweiligen Vertragsgegenstands unter einen der gesetzlichen Vertragstypen stellt bei der Erstellung eines Vertrages im IT-Bereich bereits regelmäßig die erste Herausforderung dar. Hierzu muss zunächst der konkrete Vertragsgegenstand in seiner technischen Spezifikation und Funktionsweise sowohl durch den Auftraggeber, den Softwareentwickler als Auftragnehmer, als auch den beratenden Rechtsanwalt verstanden und beschrieben werden können, damit bei der Vertragsgestaltung alle einschlägigen rechtlichen Anknüpfungspunkte erkannt und bewertet werden können. Zur Vermittlung dieses technischen Verständnisses auf der einen Seite und der nötigen rechtlichen Sensibilisierung auf der anderen Seite ist eine enge Zusammenarbeit zwischen Mandant und betreuendem Rechtsanwalt unerlässlich.

TYPENGEMISCHTE VERTRÄGE ALS REGEL IM IT-RECHT

Des Weiteren besteht die Besonderheit, dass der Vertragstyp – nachdem der Vertragsgegenstand einmal klar definiert ist – oftmals nicht eindeutig auf einen Grundtyp festgelegt werden kann. Dies folgt daraus, dass im Bereich des IT-Rechts selten nur eine alleinstehende Leistung angeboten wird. Vielmehr wird eine Mehrheit von gebündelten Einzelleistungen angeboten, welche in ihrer rechtlichen und technischen Ausgestaltung sehr verschieden sein können. Die Folge ist, dass es sich bei Verträgen im IT-Recht meist um sog. typengemischte Verträge handelt, welche mehrere Vertragstypen miteinander kombinieren.

BESONDERHEITEN BEI DER VERTRAGSGESTALTUNG

Bei der Gestaltung eines Kaufvertrages ist grundsätzlich der Sachmangelbegriff in § 434 BGB zu berücksichtigen. Ein Augenmerk im Rahmen der Prüfung der subjektiven und objektiven Beschaffenheit der Kaufsache liegt dabei im IT-Recht auf den Merkmalen der Kompatibilität, Interoperabilität und Sicherheit, welche inzwischen neu in den Gesetzestext aufgenommen wurden. Unter der Kompatibilität versteht man beispielsweise die Fähigkeit einer Sache, mit derjenigen Hardware oder Software zu funktionieren, mit welcher Sachen derselben Art in der Regel benutzt werden, wenn weder die Sache, noch die Hardware oder Software dazu verändert oder angepasst werden muss.

Ein Beispiel hierfür ist die Verwendungsmöglichkeit einer Software auf einem PC in Kombination mit einem bestimmten Betriebssystem, ohne das hierzu Änderungen am PC, dem jeweiligen Betriebssystem oder der Software erforderlich sind.

VERBRAUCHERVERTRÄGE IM IT-RECHT

Handelt es sich bei dem zu erstellenden Vertrag zudem um einen Verbrauchervertrag, d.h. einen Vertrag, der zwischen einem Unternehmer und einem Verbraucher abgeschlossen werden soll, dann sind die ebenfalls neu eingeführten Paragraphen über digitale Produkte gemäß §§ 327 ff. BGB zu beachten. Diese Vorschriften stellen keinen eigenständigen Vertragstyp dar, da sie keine Anspruchsgrundlagen für primäre Leistungspflichten enthalten und auch die Rechtsnatur der einzelnen Verträge über digitale Produkte offen lassen. Angeknüpft wird, erstmals in der Geschichte des Bürgerlichen Gesetzbuches, nicht an die Art der vereinbarten Leistung, sondern an die Art des Leistungsgegenstandes. In der praktischen Rechtsanwendung wird indes weiterhin zunächst der Sachverhalt unter die klassischen Vertragstypen eingeordnet. Erst in einem zweiten Schritt wird dann das, gemäß dem jeweiligen Grundvertragstyp geltende Recht, mit den einschlägigen Vorschriften der §§ 327 ff. BGB abgeglichen.

WERKVERTRÄGE IM IT-RECHT

Bei der Gestaltung von Werkverträgen im Rahmen der Erstellung von Individualsoftware stellt die Abnahme der Leistung einen wichtigen Regelungsbereich dar. Damit genaue Abnahmekriterien festgelegt werden können ist es zunächst unerlässlich, dass der Kunde ein vollständiges und eindeutiges Pflichtenheft erstellt und der anderen Vertragspartei pünktlich zur Verfügung stellt. Das Pflichtenheft muss hierbei diejenigen technischen Anforderungen beschreiben und festlegen, die durch die Software zwingend erfüllt werden müssen. Sofern das Pflichtenheft unvollständig, technisch fehlerhaft oder nicht im Zeitplan erstellt wurde, kann dies im Rahmen der Abnahme und des fristgemäßen Projektablaufs problematisch werden. Daher sollte die Erstellung des Pflichtenheftes im Vertrag in Gestalt von Mitwirkungspflichten des Kunden als vertragliche Nebenpflicht festgelegt sein.

DER BLICK ÜBER DEN TELLERRAND AUF ANDERE RECHTSGEBIETE

Grundsätzlich sind darüber hinaus bei einem Großteil der IT-Verträge auch die, über das allgemeine Vertragsrecht hinausgehenden Rechtsgebiete zu berücksichtigen. Dazu zählt unter anderem das Urheberrecht sowie geistige Schutzrechte wie das Patent- oder Markenrecht. Ebenso zu berücksichtigen sind datenschutzrechtliche Vorgaben aus der DSGVO, dem BDSG und dem TTDSG.

UNTERSTÜTZUNG BEI RECHTSSTREITIGKEITEN IN ZUSAMMENHANG MIT IT-VERTRÄGEN

Sofern im Rahmen der Abwicklung eines Vertragsverhältnisses im IT-Rechtsbereich über die Erfüllung von Hauptleistungs- oder Schadensersatzverpflichtungen Streit entsteht, besteht auch hier, d.h. wie im übrigen allgemeinen Zivilrecht, die Möglichkeit der außergerichtlichen oder gerichtlichen Rechtsdurchsetzung.

FAZIT

Die Gestaltung von IT- Verträgen enthält einige rechtliche Besonderheiten, die leicht zu Fallstricken in IT-Projekten werden können.

Die Exotik des IT-Vertragsrechts lässt sich jedoch beherrschen: Ein auf das IT-Recht spezialisierter Rechtsanwalt behält den Durchblick im vermeintlichen Paragraphen-Dschungel, hat die Besonderheiten im Blick und kann sowohl im Rahmen der Vertragserstellung und –beendigung, als auch bei der Rechtsverteidigung kompetent beraten und unterstützen.

Ihre Ansprechpartnerin
Chiara Bidmon
Rechtsanwältin

ChatGPT und die rechtlichen Herausforderungen beim Einsatz von KI

Disclaimer: Der vorliegende Artikel über ChatGPT wurde mit Hilfe von ChatGPT geschrieben. ChatGPT wurde angewiesen, einen juristischen Fachartikel über die rechtlichen Risiken bei der Verwendung von ChatGPT aus Sicht eines Rechtsanwalts zu schreiben. Die Stellen an denen der Autor den Text nachgepflegt oder ergänzt hat, sind farblich gekennzeichnet. Die Bildgestaltung dieser Seite wurde im Weiteren teilweise mithilfe von „Stable Diffusion" generiert, einem Deep-Learning-Text-zu-Bild-Generator.

ChatGPT erfreut sich aktuell größter Beliebtheit in der Presse und den Fachnachrichten. Chatbots wie ChatGPT werden in verschiedenen Branchen und Bereichen zunehmend eingesetzt, um Kundenanfragen und -bedürfnisse zu erfüllen und automatisieren. ChatGPT wurde durch das US-amerikanische Unternehmen Open-AI entwickelt und im November 2022 veröffentlicht. Es zielt darauf, mittels eines KI-Systems einen natürlichen Mensch-Maschine-Dialog zu ermöglichen. Diese Technologie bietet viele Vorteile, aber auch rechtliche Risiken, insbesondere in Bezug auf Schadenersatzansprüche. In diesem Artikel werden wir uns auf die rechtlichen Aspekte konzentrieren, die bei der Verwendung von ChatGPT beachtet werden sollten.

HAFTUNG DES VERWENDERS

Wenn ein Schaden auftritt, der durch den Einsatz von ChatGPT verursacht wird, haftet der Verwender des Chatbots dafür. Ein Schaden kann beispielsweise dann auftreten, wenn ChatGPT auf eine Anfrage eines Nutzers mit einer falschen oder ungenauen Antwort antwortet, was zu einem Schaden führt. In diesem Fall könnte der Chatbot-Verwender für den entstandenen Schaden haftbar gemacht werden. Der Verwender von ChatGPT sollte sicherstellen, dass die Antworten, die der Chatbot gibt, auf sachkundiger Grundlage basieren und keine falschen oder irreführenden Informationen enthalten.

Die Verwendung von ChatGPT birgt auch das Risiko von Fehlfunktionen. Der Chatbot könnte beispielsweise aufgrund von Programmierfehlern oder Datenfehlern fehlerhafte Antworten geben oder sogar ausfallen. Wenn dies zu einem Verlust oder Schaden für den Nutzer führt, könnte der Verwender von ChatGPT für den entstandenen Schaden haftbar gemacht werden.

DATENSCHUTZ UND DATENSICHERHEIT

Die Verwendung von ChatGPT kann auch Datenschutz- und Datensicherheitsrisiken mit sich bringen. Insbesondere muss der ChatGPT-Verwender sicherstellen, dass die von den Nutzern bereitgestellten Daten sicher und geschützt sind. Andernfalls könnte der Verwender von ChatGPT für Datenschutzverletzungen haftbar gemacht werden.

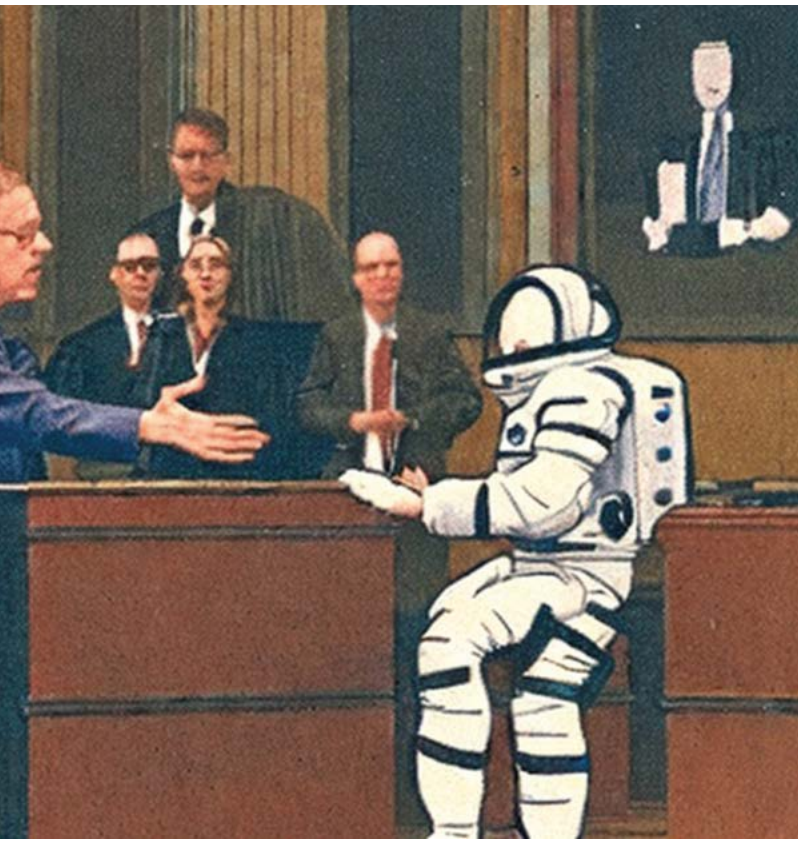
Der Chatbot-Verwender sollte sicherstellen, dass er den Datenschutzbestimmungen und Datenschutzgesetzen entspricht. Dazu gehört beispielsweise, dass der Chatbot-Verwender nur die Daten sammelt, die für die Erbringung der Chatbot-Dienste erforderlich sind, dass er die Daten nur für diesen Zweck verwendet und dass er die Daten nur solange aufbewahrt, wie dies gesetzlich zulässig ist.

ZWISCHENFAZIT:

Anhand der vorstehenden Ausführungen zeigen sich bereits die Schwächen von ChatGPT in der gegebenen Fragestellung. Es ist bislang völlig ungeklärt, ob und wie die Haftungsfolgen beim Einsatz von ChatGPT aussehen sollen. Ob bspw. eine Produkthaftung oder vertragliche Schadenersatzansprüche bei der Verwendung von ChatGPT entstehen könnten, lässt sich bisweilen nicht beantworten. Auch das Thema Datenschutz ist bislang nicht sinnvoll und im erforderlichen Umfang aufgeklärt.

„Der Verwender von ChatGPT sollte sicherstellen, dass die Antworten, die der Chatbot gibt, auf sachkundiger Grundlage basieren und keine falschen oder irreführenden Informationen enthalten."

„Die Verwendung von ChatGPT bietet viele Vorteile, aber auch rechtliche Risiken, insbesondere in Bezug auf bislang ungeklärte Haftungsfragen.“



Die italienische Regierung hat erst kürzlich die Verwendung von ChatGPT gesperrt, da rechtliche Grundlagen für die Speicherung der Daten fehlen. Auch deutsche Datenschutzbehörden haben ein förmliches Verfahren gegen OpenAI, den Betreiber von ChatGPT eröffnet, da bislang ungeklärt ist, was mit den Nutzereingaben geschieht und woher die Ausgabedaten von ChatGPT stammen.

URHEBERRECHT

Die Verwendung von ChatGPT birgt auch das Risiko der Verletzung von geistigem Eigentum oder Urheberrechten. Wenn ChatGPT beispielsweise auf urheberrechtlich geschützte Informationen zugreift, ohne die erforderlichen Genehmigungen oder Lizenzen zu besitzen, könnte der Verwender von ChatGPT für eine Urheberrechtsverletzung haftbar gemacht werden.

Der Verwender von ChatGPT sollte sicherstellen, dass er die erforderlichen Genehmigungen und Lizenzen für alle Informationen, die von ChatGPT genutzt werden, besitzt. Wenn der Chatbot Informationen verwendet, die von Dritten stammen, sollte der Betreiber eine schriftliche Erlaubnis von den Eigentümern dieser Informationen einholen.

ZWISCHENFAZIT:

Auch hier zeigen sich die Limits von ChatGPT. Während die von der Anwendung entwickelten Hinweise sicherlich wertvoll sind, erscheint es kaum praktikabel, sämtliche Lizenzen der Trainingsdaten von ChatGPT zu erwerben um ChatGPT einzusetzen. Zudem ist auch urheberrechtlich höchst umstritten ob die Texte die ChatGPT generiert selbst dem Urheberrechtsschutz unterliegen.

ZUSAMMENFASSUNG

Die Verwendung von ChatGPT bietet viele Vorteile, aber auch rechtliche Risiken, insbesondere in Bezug auf bislang ungeklärte Haftungsfragen. Um diese Risiken zu minimieren, sollte der Chatbot-Verwender sicherstellen, dass der Chatbot korrekt programmiert und getestet wurde, dass er den Datenschutzbestimmungen und Datenschutzgesetzen entspricht, dass er die erforderlichen Genehmigungen und Lizenzen für alle verwendeten Informationen besitzt und dass er ein effektives System zur Überwachung des Chatbots hat. Durch die Einhaltung dieser Richtlinien können Betreiber von Chatbots die Risiken minimieren und ihre Nutzer vor Schäden schützen.
Wir hoffen, dass dieser Artikel Ihnen geholfen hat, die rechtlichen Risiken bei der Verwendung von ChatGPT zu verstehen. Bitte beachten Sie, dass dieser Artikel keine rechtliche Beratung darstellt und Sie sich bei Fragen zu spezifischen rechtlichen Problemen an einen Anwalt wenden sollten.

FAZIT

Diese Aufforderung möchten wir aufgreifen. Wenn Sie die Implementierung von ChatGPT oder anderweitiger KI in Ihrem Unternehmen planen, unterstützen wir Sie gerne bei der Gestaltung und Implementierung zur Vermeidung rechtlicher Risiken und Haftungsansprüchen.

Ihr Ansprechpartner
Nils Stark, LL.M. (Liechtenstein)
Rechtsanwalt

KURZ UND KNAPP

SO FUNKTIONIERT EINE RECHTSKONFORME EINWILLIGUNG

„Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Über den Text des Erwägungsgrund 32 zur DSGVO ist im Grunde schon (fast) alles gesagt. Schauen wir uns den Satz daher etwas genauer an, um zu einer Checkliste für wirksame Einwilligungen zu gelangen.

Einwilligungen finden sich in vielen Situationen in unserem privaten und betrieblichen Alltag. Dabei kann jedoch längst nicht jede Einwilligung im datenschutzrechtlichen Sinn als wirksam betrachtet werden. Da eine unwirksame Einwilligung meist zu einem Fehlen des Rechtsgrundes der auf die Einwilligung gestützten Verarbeitung führt, lohnt es sich, das Thema genauer zu betrachten.

WO IST DAS THEMA DER EINWILLIGUNG GEREGELT?

Eine Begriffsbestimmung findet sich in Art. 4 Nr. 11 DSGVO, die Eignung der Einwilligung als Rechtsgrundlage der Verarbeitung folgt aus Art. 6 Abs. 1 UAbs. 1 lit. a und Art. 9 Abs. 2 lit. a DSGVO, die Bedingungen für die Einwilligung finden sich in Art. 7 DSGVO.

AN WELCHE THEMEN MUSS ICH BEI EINEM EINWILLIGUNGSERSUCHEN REGELMÄSSIG DENKEN?

- ✓ Prüfen Sie, ob neben der Einwilligung noch ein weiteres gesetzliches Verarbeitungsbefugnis in Betracht kommt.
- ✓ Beschreiben Sie den Zweck der Einwilligung und formulieren Sie den Erklärungsinhalt, d.h. die geplante Datenverarbeitung, so konkret wie möglich.
- ✓ Machen Sie sich Gedanken, ob die betroffene Person freiwillig und zwanglos einwilligen kann. Denken Sie dabei an mögliche Machtungleichgewichte, wie sie sich in einem Beschäftigungsverhältnis oder bei einem Vertragsabschluss ergeben mögen.
- ✓ Koppeln Sie die Erteilung der Einwilligung keinesfalls an die Erfüllung einer vertraglichen Leistung.
- ✓ Achten Sie darauf, dass die betroffene Person mit ihrer Einwilligung auch nachweislich über ihr Widerrufsrecht informiert wird.
- ✓ Stellen Sie sicher, dass die betroffene Person vor Abgabe der Einwilligungserklärung die Möglichkeit hat, alle gesetzlich geforderten Informationen frühzeitig zu erhalten und ihr eine ausreichende Überlegungszeit bleibt.
- ✓ Stellen Sie sicher, dass Sie nachweisen können, dass Sie die Einwilligung von der betroffenen Person erhalten haben.

WAS IST WEITERHIN ZU BEACHTEN?

In einigen Fällen, wie etwa bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 2 lit. a DSGVO), bei der Einwilligung durch Minderjährige (Art. 8 DSGVO) oder bei Einwilligungen in automatisierte Einzelentscheidungen (Art. 22 Abs. 2 lit. c DSGVO) werden weitere gesetzliche Anforderungen an Einwilligungen gestellt.
Die Themen der Checkliste dienen daher der Orientierung und sind nicht abschließend. Bei konkreten Fragen wenden Sie sich gerne an unsere Kanzlei.

Ihr Ansprechpartner
Matthias Herkert
Leiter Consulting

Rechtssicheres Reagieren? Oder rechtssicheres Reagieren!

VOM UMGANG MIT BETROFFENENANFRAGEN UND WAS SIE DAZU WISSEN SOLLTEN

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“, BVerfG 1983.

Aus dieser Grundsatzentscheidung des Bundesverfassungsgerichts ging das Recht auf informationelle Selbstbestimmung hervor, welches als eine besondere Ausprägung des Allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG gilt. Aus diesem folgt, dass jeder Person grundsätzlich das Recht zukommt, autark darüber zu entscheiden, wem sie eigene personenbezogenen Daten zur Verfügung stellen möchte.

WARUM DIESE ENTSCHEIDUNG AUCH FÜR SIE VON RELEVANZ IST? DIE RECHTE DES EINEN SIND DIE PFLICHTEN DES ANDEREN!

Die Rechte der betroffenen Person, wie sie in Kapitel 3 der Datenschutzgrundverordnung (DSGVO) niedergelegt wurden, dienen als wichtige Grundlage für die Umsetzung der informationellen Selbstbestimmung. Um ein ausreichendes Schutzniveau zu gewährleisten, sowie um drohende Geldbußen zu vermeiden, ist es essentiell, einen Leitfaden im Repertoire zu haben, welcher einen sicheren Umgang mit Betroffenenanfragen ermöglicht.

DIE WICHTIGSTEN BETROFFENENRECHTE IM ÜBERBLICK

Wie sich bereits aus Erwägungsgrund 63 S. 1 DSGVO ergibt, ist es das Recht eines jeden Betroffenen, Gewissheit hinsichtlich der Verarbeitung seiner Daten zu erlangen und so eine Rechtmäßigkeitsüberprüfung anstreben zu können. Als Instrument gibt die DSGVO dem Betroffenen mehrere Rechte zur Durchsetzung an die Hand.

Recht auf Auskunft: Art. 15 DSGVO normiert das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob dieser personenbezogene Daten des Antragstellers verarbeitet und um welche es sich handelt.

Recht auf Berichtigung: Art. 16 DSGVO ermöglicht den Betroffenen von dem Verantwortlichen unverzüglich die Berichtigung unrichtiger personenbezogener Daten zu verlangen, wobei auch die Vervollständigung bei fehlenden Daten möglich ist.

Recht auf Löschung: Art. 17 DSGVO enthält das Recht der Datenlöschung, nach welchem die betroffene Person von dem Verantwortlichen verlangen kann, sie betreffende personenbezogene Daten unverzüglich zu löschen. Gleichzeitig umfasst Art. 17 DSGVO die Verpflichtung des Verantwortlichen, die Daten unverzüglich zu löschen, sofern einer der unter Art. 17 Abs. 1 DSGVO niedergelegten Gründe eingreift.

Recht auf Einschränkung: Art. 18 DSGVO bestimmt, dass der Betroffene von dem Verantwortlichen die Einschränkung der Verarbeitung seiner Daten verlangen kann. Diese dient dem vorläufigen Interessenausgleich, mit welcher eine verschärfte Zweckbindung einhergeht. Demnach ist eine Weiterverarbeitung nur unter engen Voraussetzungen möglich.

Recht auf Datenübertragbarkeit: Art. 20 DSGVO regelt das Recht der Datenübertragbarkeit, welches die Übertragung personenbezogener Daten zwischen Datenbanken vorsieht. Dies enthält zum einen das Recht, personenbezogene Daten in einem geeigneten Format zu erhalten. Zum anderen umfasst es das Recht, die Daten an einen anderen Anbieter zu übermitteln als auch diese vom Verantwortlichen an einen anderen Anbieter übermitteln zu lassen.

Recht auf Widerspruch: Art. 21 DSGVO eröffnet dem Betroffenen die Möglichkeit gegen eine grundsätzlich zulässige Datenverarbeitung, durch die Ausübung des Widerspruchs, vorzugehen.

BETROFFENENANFRAGE UND WEITER?

Die vorgenannten Rechte können nun also Gegenstand einer Betroffenenanfrage an Ihr Unternehmen sein. Doch wie ist zu handeln, wenn eine solche Anfrage eingeht?
Für einen sicheren Umgang mit Betroffenenanfragen ist es zunächst unumgänglich, diese als solche zu identifizieren. Klingt trivial — ist es aber nicht immer. Inhaltlich werden Anfragen meist umgangssprachlich ausgestaltet sein, sodass es einer näheren Betrachtung des Anliegens bedarf. Schulen und sensibilisieren Sie Ihr Team darauf, datenschutzrechtliche Anfragen zu erkennen!
Das weitere Vorgehen orientiert sich nun an folgendem groben Ablauf:

Eingangsbestätigung senden
↓
Identitätsfeststellung
↓
Bearbeitungsbestätigung senden
↓
Identifizierung Datenbestände
↓
Überprüfung des Begehrens
↓
Ausführung des Begehrens
↓
Information an Betroffenen
↓
Dokumentation des Vorgangs

Dem gesetzlichen Grundsatz der Transparenz geschuldet sind die Informationen und Mitteilungen in präziser, transparenter sowie verständlicher und leicht zugänglicher Form abzufassen. Diese sind in einer klaren und einfachen Sprache zu halten. Weiter obliegt es Ihnen als Verantwortlichen dafür Sorge zu tragen, dass im Rahmen der Ausführung der Maßnahmen, Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

DIE SACHE MIT DER FRIST…

Ein besonderes Augenmerk ist auf die Frist des Art. 12 Abs. 3 S. 1 DSGVO sowie die jeweiligen ergänzenden bzw. abweichenden Bestimmungen zu legen. Doch warum?
Dem Wortlaut zufolge hat der Verantwortliche die Informationen über die nach Art. 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen.
Art. 16 als auch Art. 17 DSGVO modifizieren die Frist insoweit, dass diese sich auf die Maßnahme selbst beziehen, d.h. die Berichtigung bzw. die Löschung unverzüglich und somit ohne schuldhaftes Zögern zu erfolgen hat. Indem auf den Verweis — bezogen auf die flexiblere Bestimmung des Art. 12 Abs. 3 S. 1 DSGVO — verzichtet wird, statuiert dies, wie elementar diese Rechte sind. Daten bilden nicht nur das Fundament dafür, wie eine Person gesehen wird, auf ihrer Grundlage ergehen auch Entscheidungen, welche für den Betroffenen nachteilig wirken können.

STRUKTURIERTES VORGEHEN LOHNT SICH!

Die Wichtigkeit wird letztlich durch die hohe Bußgeldandrohung von bis zu 20 Mio. Euro dekretiert. Dies unterstreicht die Gewichtigkeit der Betroffenenrechte und sollte Anlass sein ein Konzept zu entwickeln, welches drohende Konsequenzen weitestgehend minimiert.

WIE LAUTET NUN DIE DEVISE? VORSICHT IST BESSER ALS NACHSICHT!

Der Umgang mit Betroffenenrechten bedarf gewisser Feinfühligkeit und einer klaren Struktur. Dies lässt sich durch organisatorische Vorkehrungen erreichen, welche die Zuständigkeit sowie den Ablauf regeln und so Rahmenbedingungen darstellen. Dies schafft Sicherheit, vor allem bei ungewöhnlichen Sachverhalten, die einzelfallabhängig zu beurteilen sind.
Gerade auch im Hinblick auf die Sicht eines Unternehmens von außen sollte auf den datenschutzrechtlichen Auftritt Wert gelegt werden. Dies dokumentiert, dass die Wahrung der Rechte auf der Agenda stehen, mithin als wichtig erachtet werden. DSGVO-konform zu agieren zeigt die Übernahme von Verantwortung, wie es bereits der Begriff „Verantwortlicher“ mit sich bringt.
Nutzen Sie die Anfragen letztlich als Chance, interne Abläufe zu optimieren. Gerne unterstützen wir Sie bei der Erstellung Ihrer Leitfäden, beraten Sie rechtssicher zur Gestaltung eines Leitfadens und unterstützen Sie im Bedarfsfall bei der Beurteilung und Erfüllung der gesetzlichen Betroffenenrechte.

Ihre Ansprechpartnerin
Marie-Luis Bufler
Juristin mit Schwerpunkt Datenschutzrecht

Hinweisgeberschutz

DIE GESETZLICHEN VERPFLICHTUNGEN UND WARUM SIE JETZT SCHON HANDELN MÜSSEN!

UM WAS GEHT ES BEIM HINWEISGEBERSCHUTZ?

Mit Umsetzung der EU-Richtlinie EU-RL 2019/1937, der sogenannten Whistleblower-Richtlinie, schaffen die europäischen Mitgliedsstaaten den lang ersehnten Schutz für Hinweisgebende. Ziel der Richtlinie ist es, Personen zu schützen, die Informationen über Verstöße gegen das EU-Recht melden. Ein nationales Hinweisgeberschutzgesetz wurde zum Redaktionsschluss jedoch noch nicht erlassen. Nach dessen Erlass sieht das Hinweisgeberschutzgesetz (HinschG) vor, dass Hinweisgebende auch bei Meldungen von Verstößen gegen nationales Recht geschützt sind. Maßgeblich sind dabei insbesondere Verstöße, die sanktionsbewehrt sind, aber auch gegen andere Gesetze, die in einem gesonderten Katalog aufgeführt sind.

WAS MÜSSEN UNTERNEHMEN JETZT TUN?

Die Whistleblower-Richtlinie verpflichtet öffentliche und private Organisationen sowie Behörden dazu, im Rahmen eines Hinweisgeberschutzsystems (Hinweisgebersytem) sichere Kanäle für die Meldung von Missständen und Gesetzesverstößen einzurichten und zu betreiben. Eingehende Meldungen müssen innerhalb einer knappen gesetzlichen Frist beantwortet, dokumentiert und auf ihre Stichhaltigkeit hin bewertet werden, um anschließend gegebenenfalls entsprechende Folgemaßnahmen, wie etwa interne Untersuchungen oder die Abgabe an eine zuständige Stelle, einzuleiten. Daneben verpflichtet der Entwurf des nationalen HinschG dazu, dass Beschäftigte, die für die Entgegennahme der Meldungen zuständig sind, regelmäßig geschult werden müssen.

BIS WANN MÜSSEN UNTERNEHMEN EIN HINWEISGEBERSCHUTZSYSTEM EINGEFÜHRT HABEN?

Für Unternehmen mit mehr als 250 Mitarbeitenden ist die Einführung eines Whistleblower-Systems bereits seit dem 17. Dezember 2021 verpflichtend. Kleine Unternehmen mit mehr als 50 Mitarbeitenden haben gemäß der EU-Richtlinie noch bis zum 17. Dezember 2023 Zeit für die Implementierung ihres Hinweisgebersystems. Dabei spielt es keine Rolle, ob das nationale HinSchG bis zu diesem Zeitpunkt erlassen wurde!

WAS SIEHT DAS GESETZ NOCH VOR?

Sowohl die EU-Richtlinie als auch der Entwurf des nationalen HinschG sehen ein absolutes Repressionsverbot gegen Hinweisgebende und eine entsprechende Beweislastumkehr vor. Das bedeutet, dass zu-

künftig der Arbeitgeber die Beweislast trägt, dass Entlassungen, Versetzungen oder Nicht-Beförderungen nicht auf der Tatsache beruhen, dass der betroffene Mitarbeitende einen Hinweis abgegeben hat. Wir prognostizieren, dass Arbeitnehmeranwälte dies ausnutzen werden, um Arbeitgeber unter Druck setzen zu können. Schon aus diesem Grund empfiehlt es sich ein entsprechendes System einzurichten.

WIE GEHEN UNTERNEHMEN AM BESTEN VOR?

Nachfolgend haben wir Ihnen unsere 4 Best-Practice zur Einführung eines Hinweisgeberschutzgesetzes und zur Erfüllung Ihrer gesetzlichen Verpflichtungen zusammengefasst.

1. Die Pflicht das Hinweisgebersystem einzuführen als Chance verstehen

Bevor ein Unternehmen ein Hinweisgebersystem einführt, sollte es prüfen, ob es gesetzlich dazu verpflichtet ist. Auch wenn keine gesetzliche Verpflichtung besteht, ist die Einführung eines Hinweisgebersystems in vielen Fällen sinnvoll. Ein effektives Hinweisgebersystem kann dazu beitragen, Missstände und Verstöße aufzudecken und das Vertrauen der Mitarbeitenden in das Management zu stärken. Es ist auch eine wichtige erste Verteidigungslinie für Unternehmen, da Missstände oder Gesetzesverstöße oft intern gar nicht vollumfänglich bekannt sind. Verstöße gegen Gesetze, die vom Hinweisgeberschutzgesetz umfasst sind, können schwerwiegende Straftat- oder Bußgeldtatbestände nach sich ziehen, sodass durch eine frühe Kenntnis das Risiko für Unternehmen verringert werden kann.

2. Frühzeitig und langfristig planen

Die Implementierung eines Hinweisgebersystems erfordert eine sorgfältige Planung. Unternehmen müssen sich entscheiden, ob sie eine interne Lösung oder eine Auslagerung an Dritte in Form der Ombudsstelle vornehmen wollen. Eine Beauftragung einer externen Rechtsanwaltskanzlei als Ombudsstelle wirkt sich hier meist positiv auf das Vertrauen und die Akzeptanz der Hinweisgebenden aus. Unternehmen müssen auch entscheiden, ob sie sich neben der Umsetzung der gesetzlichen Regelungen zusätzlich für eine Zertifizierung nach ISO 37002 entscheiden möchten. Es ist wichtig, dass Unternehmen hier strategisch planen und die Bearbeitung der Hinweise auf bestimmte Personen beschränken. Nur Mitarbeitende mit einer langfristigen Beschäftigungsperspektive im Unternehmen sollten das Hinweisgebersystem betreuen. Auch die Einbindung der Verpflichtungen aus dem Lieferkettengesetz kann sinnvoll vorgenommen werden.

3. Technische / organisatorische Voraussetzungen schaffen

Um ein effektives Hinweisgebersystem zu implementieren, müssen Unternehmen die notwendigen technischen und organisatorischen Voraussetzungen schaffen. Eine internetbasierte Portallösung ist nicht zwingend erforderlich, aber einfach umzusetzen. Es ist wichtig sicherzustellen, dass die Anonymität der Hinweisgebenden gewahrt wird und dass die Datenschutzkonzeption des Hinweisgebersystems angepasst wird. Die Dokumentation der Meldungen muss sichergestellt werden, damit die Meldungen dauerhaft abrufbar sind. Unternehmen sollten auch sicherstellen, dass die zuständige Meldestelle für persönliche Zusammenkünfte bereit ist, indem entsprechende vertrauliche Räumlichkeiten zur Verfügung gestellt werden.

4. Kommunikation an Stakeholder des Unternehmens

Nachdem ein verbindlicher Verhaltenskodex und eine transparente Whistleblower-Policy erstellt wurden, sollten die Prozesse zum Hinweisgebersystem transparent an die jeweiligen Stakeholder kommuniziert werden. Ein einfacher Aushang in der Mitarbeiterkantine reicht dabei nicht aus, genauso wenig wie eine Rundmail an alle Beteiligten. Es empfiehlt sich, die Prozesse zum Hinweisgebersystem bereits im Onboarding-Prozess neuer Mitarbeiter zu kommunizieren und Schulungen durchzuführen. Dabei sollten Fragen wie „Was darf gemeldet werden?“, „Wo soll gemeldet werden?“, „Wer hat Zugriff auf die Meldung?“ und „Welche Vorteile habe ich als Mitarbeiter, eine Meldung abzugeben?“ beantwortet werden. Beispiele können dabei helfen, die Schulung anschaulicher zu gestalten. Es sollte zudem klargestellt werden, dass das Hinweisgebersystem kein Kummerkasten ist und Beschwerden z.B. über das Essen auf der Weihnachtsfeier keinen Platz im Hinweisgebersystem haben.

FAZIT

Die Einführung eines Hinweisgebersystems kann für Unternehmen eine Herausforderung darstellen. Es erfordert eine vorausschauende Planung, klare Kommunikation und Schulung der Mitarbeiter, sowie die Erstellung klarer Prozesse. Wenn jedoch ein gut durchdachtes Hinweisgebersystem implementiert wird, können Unternehmen von einem verbesserten Risikomanagement und einem besseren Schutz vor Reputationsverlusten profitieren. Zudem wird das Vertrauen der Mitarbeiter in das Unternehmen gestärkt, da sie wissen, dass ihre Bedenken und Meldungen ernst genommen werden.
Bei der Umsetzung der Verpflichtungen zum HinschG können wir Sie gerne mit unserer eigenen Portallösung unterstützen. Sie finden unser Hinweisgeberportal auf unserer Website oder unter https://hinweisportal.reichert-reichert.de/. Durch die PGP-Verschlüsselung, die Möglichkeit das Portal unter eigenem Coporate Design zu betreiben und die Betreuung durch spezialisierte Rechtsanwälte und Juristen, bieten wir Ihnen eine einfache, kostengünstige und sofort implementierbare maßgeschneiderte Lösung für Ihr Unternehmen an. Gerne unterbreiten wir Ihnen eine entsprechende Paketlösung.

Ihr Ansprechpartner

Nils Stark, LL.M. (Liechtenstein)
Rechtsanwalt

E-Commerce und Rechtsanwalt – gemeinsam zum erfolgreichen Online-Shop

Welche rechtlichen Besonderheiten müssen bei der Konzeption eines Online-Shops berücksichtigt werden? Nachfolgend klären wir, wie der Rechtsanwalt in den verschiedensten Stadien der Gestaltung eines Online-Shops unterstützen kann.

GRUNDLEGENDE HERAUSFORDERUNGEN UND ANFORDERUNGEN

Die Gestaltung eines Online-Shops unterliegt einer Vielzahl von Interessen und Zielen die damit verfolgt werden sollen. Dazu zählen unter anderem die Verwirklichung von Umsatzzielen, die (Neu-) Vermarktung eines Produktes oder einer Dienstleistung, die Gewinnung von Erkenntnissen zum Käuferverhalten und der Interessentenstruktur wie auch die Erweiterung der Vertriebskanäle. Diese überwiegend wirtschaftlich geprägten und marketingorientierten Interessen sind mit den, sich im Bereich E-Commerce aus den einschlägigen Gesetzen ergebenden, rechtlichen Vorgaben in Einklang zu bringen.

Zudem müssen bei der technischen Gestaltung des Online-Shops vielfach rein praktische Faktoren berücksichtigt werden, wie beispielsweise eine einfache und übersichtliche Navigation im Online-Shop, die Bereitstellung diverser Suchfunktionen für ein schnelles Auffinden sowie die Möglichkeit der Bedienung des Online-Shops sowohl am PC als auch am Smartphone und anderen Mobile Devices. Daneben sind stets datenschutzrechtliche und allgemein zivilrechtliche Vorgaben einzuhalten und mit in die Gestaltung zu integrieren.

VORKONZEPTION DES ONLINE-SHOPS

Der Rechtsanwalt kann innerhalb aller Phasen der Entwicklung eines Online-Shops unterstützend und initiativ beratend tätig sein, so auch in der Phase der Vorkonzeption, welche im Rahmen der Festlegung des Projektziels, des Ablauf- und Terminmanagements sowie des Ressourcen- und Kostenmanagements stattfindet.

Hierbei kann der Rechtsanwalt bei der Aufsetzung eines Online-Shops von Grund auf bei der Beantwortung der folgenden Fragen unterstützen: Wird der Online-Shop sowohl von Verbrauchern als auch von Unternehmern auf Kundenseite genutzt? Wie soll der Vertragsschluss über das Online-Warenkorbsystem im Zusammenspiel mit dem anschließenden Versand einer Empfangs- oder Bestellbestätigung erfolgen?

ERSTELLUNG DER ERFORDERLICHEN RECHTLICHEN DOKUMENTE

Durch die aktive Einbindung eines Rechtsanwalts in die (ggfs. auch agile) Projektstruktur können die, das Projekt in rechtlicher Hinsicht flankierenden Dokumente, zeitgleich zur Weiterentwicklung des Projekts in technischer Hinsicht, nach Abschluss einer jeweiligen Entwicklungsphase frühzeitig entworfen, angepasst und weiterentwickelt werden. Der Rechtsanwalt arbeitet dabei eng zusammen mit den Web- und Shopdesignern, dem Datenschutzbeauftragten, dem Informationssicherheitsbeauftragten und dem Software-Entwickler-Team.

Die für das konkrete Projekt erforderlichen rechtlichen Dokumente variieren dabei je nach Umfang des Online-Shops, der verkauften Waren- oder Dienstleistungen oder der Produktbranche. In jedem Fall erforderliche Dokumente sind Allgemeine Geschäftsbedingungen, welche in der Regel auch die Zahlungsbedingungen und eine Widerrufsbelehrung für Verbraucher beinhalten sowie zusätzlich, separat die Versand- und Lieferbedingungen.

TECHNISCHE UND RECHTLICHE GESTALTUNG

Aus dem Bürgerlichen Gesetzbuch (BGB) ergeben sich für die Ausgestaltung des Online-Shops in technischer und inhaltlicher Hinsicht klare rechtliche Vorgaben, welche der Gesetzgeber im Jahr 2022 sowohl betreffend den gegenüber Unternehmern als auch gegenüber Verbrauchern bestehenden Informationspflichten im Rahmen des Vertragsschlusses im elektronischen Geschäftsverkehr nochmals verschärft hat.

Im Rahmen der sog. „Button-Lösung“ ist zunächst in Online-Shops zwingend die Bestellung über eine Schaltfläche (sog. Button) zu ermöglichen, welche ausschließlich mit dem Text „Jetzt kaufen“ oder „Zahlungspflichtig bestellen“ bezeichnet werden darf. Diese Vorgabe hat ihren Ursprung darin, dass der Käufer möglichst prägnant darauf hinzuweisen ist, dass durch die Betätigung des Buttons eine rechtsverbindliche Erklärung in den Rechtsverkehr abgegeben wird.

Ebenfalls gesetzlich vorgeschrieben ist in diesem Zusammenhang die Information des Kunden über die für den Vertragsschluss im elektronischen Geschäftsverkehr wesentlichen Informationen gemäß § 312 i und j BGB. Hierunter fällt beispielsweise die Angabe der wesentlichen Eigenschaften der Waren oder Dienstleistungen, die Angabe des Gesamtpreises einschließlich aller Steuern und aller ggfs. zusätzlich zum Gesamtpreis anfallenden Versandkosten sowie die Angabe der Zahlungs-, Liefer- und Leistungsbedingungen. Diese Informationen müssen dem Kunden möglichst vollständig vor der Einleitung des Bestellvorgangs, d.h. vor dem Einlegen der Ware in den digitalen Warenkorb, zur Verfügung gestellt werden und können darüber hinaus unmittelbar bevor der „Jetzt-Kaufen-Button“ betätigt wird, d.h. im Rahmen der Bestellübersicht in klarer, verständlicher und hervorgehobener Weise zusammengefasst zur Verfügung gestellt werden.

Dem Kunden muss im Rahmen der Bestellübersicht auch die Möglichkeit der Korrektur oder Löschung einzelner Bestellungen aus dem Warenkorb gegeben werden. Zudem ist die Art und Weise der technischen Einbindung von Allgemeinen Geschäftsbedingungen im Rahmen der Bestellung, und damit die wirksame Einbeziehung der Allgemeinen Geschäftsbedingungen in den Vertrag, entscheidend.

Im Rahmen der Neugestaltung des Bürgerlichen Gesetzbuchs wurde in Gestalt von § 312 k BGB auch die Verpflichtung des Online-Shop-Betreibers eingeführt, dass bei einer Ermöglichung eines Vertragsschlusses durch einen Verbraucher im elektronischen Geschäftsverkehr, welcher die Begründung eines Dauerschuldverhältnisses zum Gegenstand hat, ein sog. Kündigungsbutton zur Verfügung zu stellen ist. Über diesen Button muss dem Verbraucher eine unkomplizierte Möglichkeit zur Verfügung gestellt werden, wie der Vertrag auf demselben, elektronischen Wege gekündigt werden kann, wie der Vertrag zuvor geschlossen wurde.

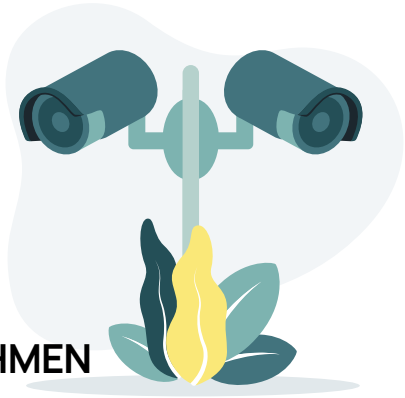
DATENSCHUTZ & CO.

Im Zuge der Gestaltung des Online-Shops sollte auch die Erstellung der gemäß Art. 13 DSGVO erforderlichen Datenschutzinformationen, die Umsetzung der gemäß Art. 32 DSGVO geforderten Maßnahmen zur Datensicherheit sowie die Erstellung einer Cookie-Richtlinie und eines Cookie-Banners, welche nach dem neuen Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Verbindung mit der DSGVO erforderlich sind, nicht außer Acht gelassen werden.

FAZIT

Bei der Gestaltung eines Online-Shops sind in rechtlicher Hinsicht einige gesetzliche Vorgaben zu berücksichtigen, welche durch einen auf das IT-Recht spezialisierten Rechtsanwalt rechtskonform, praxisnah und anwenderfreundlich umgesetzt werden können.
Wir unterstützen Sie gerne hierbei!

Ihre Ansprechpartnerin
Chiara Bidmon
Rechtsanwältin



KURZ UND KNAPP

SO FUNKTIONIERT EINE RECHTSKONFORME VIDEOÜBERWACHUNG IM UNTERNEHMEN

Die Anforderungen an eine zulässige Videoüberwachung im Unternehmen sind vielfältig und die gesetzlichen Vorschriften des Datenschutzrechts sind in der Praxis nicht immer leicht verständlich und umsetzbar. In unserer Rubrik „KURZ UND KNAPP" zeigen wir Ihnen, wie der Einstieg in das Thema dennoch rasch und rechtssicher gelingen kann.

Eine Videoüberwachung im Unternehmen erzeugt unter Umständen einen massiven Überwachungs- und Anpassungsdruck bei den betroffenen Menschen und ist daher regelmäßig unzulässig. Um eine zulässige Videoüberwachung zu erreichen und drohende Geldbußen von bis zu 20 Mio. Euro zu vermeiden, lohnt es daher, vor der Inbetriebnahme genau zu planen und sich rechtlich beraten zu lassen.

AUF WELCHER RECHTSGRUNDLAGE IST EINE VIDEOÜBERWACHUNG IM UNTERNEHMEN ZULÄSSIG?

Die Zulässigkeit von Videoüberwachungen in Unternehmen richtet sich regelmäßig nach den Vorschriften der Datenschutz-Grundverordnung (DSGVO). Da die DSGVO hierbei keine speziellen Regelungen für den Einsatz von Videotechnik enthält, müssen Verarbeitungen meist auf das berechtigte und überwiegende Interesse des Unternehmens aus Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gestützt werden.

IN WELCHEN FÄLLEN IST EINE VIDEOÜBERWACHUNG IM UNTERNEHMEN ZULÄSSIG?

Die Zulässigkeit ist immer vom konkreten Zweck im Einzelfall abhängig. Häufige Zwecke im betrieblichen Bereich sind die präventive Verhinderung von Einbrüchen, Diebstählen und Vandalismus, der Schutz und die Abwehr unbefugten Betretens, die Verhinderung von Übergriffen auf Personal oder die Beweissicherung zur Durchsetzung von Rechtsansprüchen.

WANN IST EINE VIDEOÜBERWACHUNG IM UNTERNEHMEN IMMER UNZULÄSSIG?

Die Intim- oder Persönlichkeitssphäre von Personen darf auch im Arbeitsverhältnis nicht verletzt werden. Ein Kameraeinsatz in sensiblen Bereichen wie Umkleidekabinen, Sanitär-, Pausen-, Sozial- und Aufenthaltsräumen ist daher unzulässig. Auch die Videoüberwachung von Beschäftigten an ihren Arbeitsplätzen oder in Pausenräumen ist ganz regelmäßig nicht zulässig.

WIE KANN SICHERGESTELLT WERDEN, DASS EINE VIDEOÜBERWACHUNG RECHTSSICHER IST?

Orientieren Sie sich zur Planung einer Videoüberwachung an unserer nachstehenden Checkliste und holen Sie sich mit diesen Unterlagen bei Unsicherheiten rechtliche Beratung und Unterstützung ein.

- ✓ Legen Sie den tatsächlichen Zweck der Videoüberwachung schriftlich fest.
- ✓ Schreiben Sie auf, warum dieser Zweck nur durch eine Videoüberwachung sinnvoll erreicht werden kann.
- ✓ Notieren Sie, warum Ihr Interesse an der Videoüberwachung objektiv wichtiger ist als die Persönlichkeitsrechte der überwachten Personen.
- ✓ Legen Sie den Bereich fest, der überwacht werden soll und die Zeiträume der Überwachung.
- ✓ Verpixeln Sie Bereiche, die nicht unbedingt erfasst werden müssen oder in denen eine Erfassung schlicht unzulässig ist.
- ✓ Notieren Sie, wie lange die Videos gespeichert werden müssen und stellen Sie sicher, dass alle Aufzeichnungen anschließend unverzüglich gelöscht werden.
- ✓ Überlegen Sie, ob eine Datenschutz-Folgenabschätzung erforderlich ist und notieren Sie diese Überlegung.
- ✓ Bringen Sie vollständige Hinweise auf die Videoüberwachung so an, dass die Betroffenen vor Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen können.
- ✓ Legen Sie schriftlich fest, welche Personen unter welchen Voraussetzungen auf die Aufzeichnungen zugreifen dürfen und wie diese Zugriffe protokolliert werden.
- ✓ Stellen Sie technisch und organisatorisch sicher, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Aufzeichnungen gewährleistet ist.

Als abschließender Hinweis: die Themen der Checkliste dienen der Orientierung und sind selbstverständlich nicht abschließend. Ihre Beantwortung führt nicht automatisch zur Zulässigkeit der Videoüberwachung. Bei konkreten Fragen zur Videoüberwachung können Sie sich gerne an unsere Kanzlei wenden.

Ihr Ansprechpartner
Matthias Herkert
Leiter Consulting

TTDSG: Neue Cookie-Regeln für Ihre Website

Jede Website braucht sie: Die Datenschutzinformation. Sie soll einen transparenten und leicht verständlichen Überblick über den Umgang mit personenbezogenen Daten von Besuchern und Nutzern der Website geben. Werden über eine Webanalyse Nutzerprofile erstellt, dann ist die transparente Information und die leicht verständliche Darstellung der dafür verwendeten Cookies zudem zwingender Teil der Datenschutzinformation.

TTDSG WER?

War im Hinblick auf Cookies zum Tracking und sonstigen Webanalyse bisher nur die DSGVO einschlägig, sieht sich der Websitebetreiber mit dem neuen TTDSG (Telekommunikation-Telemedien-Gesetz), das seit Dezember 2021 in Kraft ist, vor neue Aufgaben gestellt. Das TTDSG hakt dort ein, wo ein Cookie (oder eine vergleichbare Technologie) auf dem Endgerät des Nutzers Platz nimmt und Daten ausliest, diese Daten jedoch nicht zwingend personenbezogen sein müssen. Ganz so als würde jemand ungefragt während Ihrer Abwesenheit Ihre Wohnung betreten und sich umsehen wie Sie eingerichtet sind.

COOKIES UND ANDERE TRACKING-TOOLS

Nutzt eine Website z. B. Cookies, um über ein Tracking oder sonstige Webanalyse personenbezogene Daten zur Erstellung von Nutzerprofilen zu sammeln, so durfte die Verarbeitung nach DSGVO ausschließlich mit der Einwilligung der Nutzer geschehen. Eine Ausnahme vom Einwilligungserfordernis besteht nur dann, wenn die Cookies für den Betrieb der Website technisch notwendig sind. Bereits unter der DSGVO war es bisher sinnvoll, sich vom Programmierer helfen zu lassen und ein Cookie-Verzeichnis zu erstellen, das Informationen über den Namen, den Anbieter, den Zweck und die Laufzeit eines jeden (!) Cookies beinhaltet. Unter dem neuen TTDSG ist erneut Fleißarbeit gefragt. Nehmen Sie erneut Ihren Programmierer und das Cookie-Verzeichnis zur Hand und werfen Sie nun auch einen Blick auf diejenigen Cookies, die keine personenbezogenen Daten verarbeiten. Sie haben solche Cookies gefunden, die darüber hinaus nicht technisch notwendig sind? Hervorragend! Im nächsten Schritt nehmen Sie auch diese in Ihr Cookie-Banner auf und holen sich auch für diese Cookies eine Einwilligung der Nutzer ein, bevor sie auf deren Endgerät gesetzt werden.

ZUSAMMENFASSUNG

Das TTDSG schließt eine rechtliche Lücke dort, wo der Anwendungsbereich der DSGVO endet (keine Verarbeitung personenbezogener Daten) und Technologien von Websitebetreibern dennoch dafür sorgen, dass Nutzerprofile auch über nicht-personenbezogene Daten erstellt werden können (z. B. Fingerprints, Pixel und zukünftige Tracking-Technologien). Ausnahmen gelten für technisch erforderliche Cookies und andere technisch erforderliche Technologien. Eine Revision der eigenen Website ist dringend empfohlen, nicht zuletzt da Verstöße sowohl nach der DSGVO als auch nach dem TTDSG mit Sanktionen belegt werden können.

Cookies und andere Tracking-Tools sind zwar ein wesentlicher, aber eben nur ein Teil einer Websiteprüfung. Weitere Punkte, die bei der Erstellung oder Pflege einer Website beachtet werden sollten, finden Sie auf unserem Blog in dem Artikel „Die Datenschutzerklärung auf der Homepage“.

Ihre Ansprechpartnerin
Eileen Binder
Wirtschaftsjuristin, LL.B.

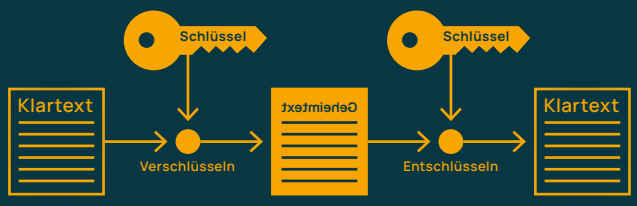
VERSCHLÜSSELUNG, HASHING UND KRYPTOGRAFISCHE VERFAHREN FÜR DIE HOSENTASCHE

Der Einsatz kryptographischer Verfahren wird in Gesetzen und Normen zum Datenschutz und zur Informationssicherheit ausdrücklich gefordert. Dabei scheint das Thema meist komplex und unverständlich. Ist Kryptographie also nur etwas für Experten oder helfen die Verfahren uns allen, den Umgang mit Daten und Informationen im Alltag sicherer zu machen?

Artikel 32 Abs. 1 lit. a DSGVO benennt die Verschlüsselung personenbezogener Daten als eine Möglichkeit, bei Datenverarbeitungen ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Und auch in der ISO/IEC 27001:2022 wird in Control 8.24 gefordert, dass Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.
Schauen wir also mal genauer hin.

WAS IST VERSCHLÜSSELUNG EIGENTLICH?

Unter Verschlüsselung versteht man Verfahren, die Daten aus einem Klartext mittels eines Schlüssels in eine nicht mehr lesbare Form, den sogenannten Geheimtext, umwandeln.
Das klingt erst einmal einfach und im Grunde ist es das auch!



WIE SIEHT EINE EINFACHE VERSCHLÜSSELUNG AUS?

Betrachten wir die Idee an einem Beispiel:
Wir haben ein Zahlenschloss, in dem die drei Ziffern beim ersten Versuch in der richtigen Reihenfolge eingestellt werden müssen. Wenn wir uns die richtige Nummernfolge (395) auf einem Blatt Papier notieren, kann jeder, der das Blatt findet, das Schloss öffnen.

Um dies zu verhindern, denken wir uns einen Schlüssel aus, der Ziffern durch Zeichen ersetzt:

1 = %	2 = *	3 = §	4 = ,	5 = $
6 = [	7 = „	8 = ?	9 = #	0 = }

Diesen Schlüssel wenden wir nun auf die Nummernfolge des Schlosses an:
3 = § 9 = # 5 = $

Aus dem Klartext 395 wird so der Geheimtext §#$. Das Anwenden des Schlüssels auf den Klartext bezeichnet man als Verschlüsselungsalgorithmus.
Jede Person, der wir unseren Schlüssel geben, wird aus den drei Zeichen ohne Weiteres die Ziffernfolge des Schlosses ablesen können. Ohne den Schlüssel wird das indes schwer.

IST DAS WIRKLICH SICHER?

Wie so oft im Leben — es kommt darauf an! Der Anspruch an ein Verschlüsselungsverfahren hängt davon ab, was mit der Verschlüsselung geschützt werden soll und wer ihr „Gegner" ist.
Hängt das Nummernschloss aus unserem Beispiel an einem Fahrrad, kann der entwickelte Schlüssel auf einem Schulhof völlig ausreichend sein. Hängt das Nummernschloss an Ihrer Haustüre, mag die Verschlüsselung bereits einem vernünftigen Sicherheitsgefühl entgegenstehen und hängt das Nummernschloss online vor Ihrem Bankkonto, dürfen Sie davon ausgehen, dass der zuvor entwickelte Schlüssel bei einem Hacking nur wenige Sekunden hält.

VERSCHLÜSSELN IST EIN KRYPTOGRAFISCHES VERFAHREN

Kryptografische Verfahren dienen dazu, Daten und Informationen vor unbefugtem Zugriff zu schützen und einen sicheren Austausch von Daten und Informationen zu ermöglichen.
Unter die kryptographischen Verfahren fallen neben der Verschlüsselung auch Hashfunktionen. Anders als Verschlüsselungen sind Hashwerte nicht invertierbar, können also nicht mehr in ihren Ursprungswert zurückgerechnet werden. Auch die Idee dahinter ist einfach. Während es in der Verschlüsselung darum geht, einen Klartext zu verschlüsseln, damit Dritte ihn nicht lesen können, der Empfänger ihn jedoch durch Entschlüsselung wieder lesbar macht, geht es beim Hashing darum, einen Klartext in einen Geheimtext zu übertragen, ohne

diesen jemals wieder zu entschlüsseln.
Hashfunktionen und die mittels dieser ermittelten Hashwerte sind daher für Passwörter gut geeignet, da ein Zurückrechnen weder notwendig noch gewollt ist. Die Korrektheit des Passwortes kann ohne weiteres durch den Vergleich des berechneten mit dem gespeicherten Hashwert verifiziert werden.

AUS EINEM PASSWORT WIRD EIN HASHWERT

Lassen Sie uns auch diesen Schritt an einem Beispiel betrachten. Hierzu benötigen Sie nun die r&r-Passwortkarte, die wir Ihnen auf unser Kanzleimagazin aufgeklebt haben (auf Ihrem Magazin klebt keine Passwortkarte? Kein Problem! Rasch eine Mail an passwortkarte@reichert-reichert.de senden).
Für unser Beispiel gehen wir davon aus, dass aus einem unsicheren, jedoch leicht zu merkenden Passwort beliebiger Länge, ein sicheres Passwort mit einer festen Länge von 12 Zeichen erzeugt werden soll.

WIE FUNKTIONIERT EINE PASSWORTKARTE?

Sie ahnen es schon – die Idee ist einfach. Die Karte fungiert als Schlüssel, der den Klartext in den Geheimtext (= Hashwert) umwandelt. Hierzu überlegen Sie sich zuerst ein Schema, nach welchem Sie die Passwörter auf der Karte ablesen werden.

Beispiel eines Schemas: Für jeden Buchstaben des Wortes, das Sie verschlüsseln wollen, lesen Sie zwei Zeichen nach rechts auf der Karte ab. Fehlen dann noch Zeichen zur Ziellänge des Passworts (12 Zeichen), werden diese einfach von unten rechts auf der Karte aufgefüllt. Sind es zu viele Zeichen, hören Sie einfach bei 12 auf. Lautet Ihr Passwort für Ihren eMail-Account schlicht „eMail“, so ergibt sich

E = P)
M = eV
A = 4=
I = Fw
L = @3

Die noch fehlenden zwei Zeichen lesen Sie aus der unteren rechten Ecke von links nach rechts ab:
Zeile 12 = REST = ‹+

Aus dem wohl zugegebenermaßen unsicheren Passwort „eMail“, wird das neue Passwort (d.h. der Hashwert) „P)eV4=Fw@3‹+“.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	b	›	C	5	P	)	G	%	a	C	_	(	3	j	(	~	]	j	D	9	G	?	%	N	A	d
2	L	B	%	V	}	=	k	k	T	1	U	,	e	V	:	e	y	*	n	c	]	.	L	k	2	9
3	4	=	D	*	+	$	7	m	&	!	f	i	Ä	#	p	%	b	N	,	g	p	8	3	=	s	:
4	›	L	?	R	4	z	ü	3	F	w	}	B	/	ü	t	C	?	E	v	1	F	§	g	ö	&	*
5	§	9	B	,	8	g	h	+	‹	c	E	@	3	7	E	a	D	*	t	T	&	b	%	e	i	7
6	1	!	G	-	Z	~	(	8	!	m	#	i	p	+	-	j	f	‹	X	/	t	5	o	=	4	5
7	!	L	{	!	4	X	v	1	?	%	d	S	@	p	t	3	n	#	+	t	E	n	„	a	q	1
8	€	k	z	r	3	9	]	R	n	,	#	5	X	w	3	u	?	3	:	!	c	S	‹	P	ä	7
9	s	r	§	*	4	v	g	-	m	2	r	-	b	E	6	#	V	1	c	W	(	e	§	5	w	!
10	4	~	Ä	v	D	1	‹	D	/	j	-	5	;	#	T	e	7	+	B	‹	K	›	p	4	:	B
11	r	b	5	J	L	r	@	u	P	[	W	4	6	‹	!	o	Ü	p	#	7	D	v	F	v	§	p
12	:	E	b	4	e	b	(	$	s	L	1	G	k	+	R	8	3	f	*	:	w	D	#	4	‹	+

1. Einstiegspunkt & Endpunkt wählen **2.** Verlauf merken
reichert & reichert – Ihre Kanzlei in Singen und Konstanz

Fällt die Passwortkarte einer anderen Person in die Hände, kann diese ohne Ihr Schema nicht auf Ihre Passwörter schließen. Wird ihr Passwort im Klartext einer anderen Person bekannt, kann diese ohne die Passwortkarte und Ihr Schema ebenso nicht auf Ihr Passwort schließen.
Und wenn Sie Ihre Passwortkarte nun noch in Ihre Hostentasche stecken, haben wir das in unserer Überschrift zu diesem Artikel genannte Ziel erreicht und haben ein

kryptografisches Verfahren für die Hosentasche.

Interesse am Thema Datenschutz durch Datensicherheit und an der Organisation einer praxisnahen Datensicherheitsorganisation? Sprechen Sie uns an!

Ihr Ansprechpartner
Matthias Herkert
Leiter Consulting

Die Revision der ISO/IEC 27001:2022

Die im Oktober 2022 veröffentlichte ISO/IEC 27001 in der Version 2022 löst die ISO/IEC 27001:2013, die wohl wichtigste und verbreitetste Norm zur Informationssicherheit ab.

Bei der ISO/IEC 27001 handelt es sich um die wohl international führende Norm für Informationssicherheits-Managementsysteme (ISMS) und damit um den derzeit verbreitetsten Standard zur Cyber-Security-Zertifizierung. Entsprechend gespannt warteten sicherlich fast alle Anwender der Norm auf die Revision der Struktur und Vorgaben.
Im Oktober 2022 veröffentlichte das International Accreditation Forum (IAF) nun mit der ISO/IEC 27001:2022 die neue und verbesserte Nachfolge der bisher geltenden ISO 27001:2013.

ZUKÜNFTIG „NUR NOCH" 93 CONTROLS

Mit nunmehr „nur noch" 93 statt 114 Controls, einer zeitgemäßen Verschlagwortung und vier statt wie bislang 14 Abschnitten, wird die Norm formal kompakter und richtet sich auf die Herausforderungen der Cybersicherheit aus.
Dabei wurde jedoch nur eine Vorgabe gelöscht, die übrigen Kürzungen gründen in Zusammenfassungen von 56 auf 24 Sicherheitsmaßnahmen. 11 Maßnahmen kamen überdies neu hinzu.

ISO/IEC 27001:2022 ODER ISO/IEC 27001:2013 – WANN GILT WAS FÜR WEN?

Nach der Veröffentlichung der ISO/IEC 27001:2022 am 25. Oktober 2022 kann ein Erstzertifizierungsaudit nach der bisherigen ISO/IEC 27001: 2013 letztmalig im Oktober 2023 erfolgen. Eine Akkreditierung nach ISO/IEC 27001:2022 ist ab dem 25. April 2023 möglich. Bestehende Zertifikate müssen innerhalb der Transitionsphase mit einer Frist von drei Jahren bis spätestens 24. Oktober 2025 auf die neuen Anforderungen und Vorgaben umgestellt werden.

WAS IST KONKRET ZU TUN?

- Ermitteln Sie den Zeitpunkt, zu dem Sie Ihr ISM-System umgestellt haben müssen.
- Überprüfen Sie den Umfang der bereits erreichten Erfüllung der neuen Forderungen durch Ihr vorhandenes ISM-System.
- Überprüfen Sie, ob ihr ISMS alle erforderlichen Wirksamkeitsnachweise umfasst.
- Projektieren Sie die notwendigen Anpassungen aus der Lückenanalyse und aus den neuen Anforderungen der Norm.
- Schulen Sie alle Anwender Ihres ISMS zu den neuen Anforderungen und den Änderungen.

FAZIT

Mit der ISO/IEC 27001:2022 liegt eine moderne und praxisnahe Nachfolge der ISO/IEC 27001:2013 vor. Neben der Weiterentwicklung der bisherigen Handlungsfelder fördert die Revision insbesondere auch die Berücksichtigung neuer Risiken, die noch stärkere Gestaltung integrierter Managementsysteme sowie die Berücksichtigung zunehmender Compliance-Anforderungen.
Diese Herausforderung bietet die Chance, die Resilienz der betrieblichen Informationssicherheit gegenüber situativen Störungen und Bedrohungen zu überprüfen und zu erhöhen und neue, wie auch veränderte Risiken noch stärker in den Fokus zu nehmen.

Der Datenschutz rückt in den Titel der ISO/IEC 27001:2022 auf
Während die Norm bislang im Titel noch Anforderungen an „Informationstechnologie, Sicherheitsverfahren und Informationssicherheitsmanagementsysteme" erfasste, greift die Neufassung nun weiter und umfasst „Informationssicherheit, Cybersicherheit und Datenschutz". Neben der Informationssicherheit der Unternehmenswerte rückt nun also auch der Schutz personenbezogener Daten und die kooperative Umsetzung beider Aspekte in den Fokus der Norm auf.

Ihre Ansprechpartnerin
Lisa-Sabrina Thum
Bachelor of Arts, Qualitätsmanagement-Auditorin, IT-Sicherheitsbeauftragte

Informationssicherheitssysteme in kleinen und mittelständischen Unternehmen

Informationssicherheitssysteme sind in Konzernen längst alltäglich. Die Situation in kleinen und mittelständischen Unternehmen sieht noch ganz anders aus. Warum ist das so und sind Informationssicherheitssysteme auch für den Mittelstand sinnvoll?

Während ein technischer Basisschutz wie etwa Virenscanner, Firewall, Datensicherungen und Patch-Management heute in fast allen Unternehmen zum Standard der Informationssicherheit gehören, fehlt es gerade bei kleineren und mittelständischen Unternehmen meist noch immer an einer flankierenden Dokumentation wie auch an einem risikobasierten Ansatz zur Auswahl der sinnvollen IT-Sicherheitsmaßnahmen. Dabei zeigen Umfragen u.a. des BSI und der BITKOM immer wieder auf, dass die Bedeutung des Schutzes von Informationen gerade auch im Mittelstand hoch bewertet wird und die Risiken z. B. durch Hacking, Malware, Phishing oder Ransomware gesehen und ihre taktische Bedeutung als Bestandsrisiko ernst genommen werden.

HINDERNISSE FÜR DIE EINFÜHRUNG VON INFORMATIONSSICHERHEITS-SYSTEMEN IM MITTELSTAND

Wesentliche Gründe für den Verzicht auf die Dokumentation der Systeme zur Informationssicherheit sind häufig der erwartete personelle und zeitliche Aufwand für den Aufbau. Weiterhin wirkt auch der formalisierte Aufbau „typischer" Informationssicherheitssysteme wie des IT-Grundschutzes nach BSI oder der ISO-Sicherheitsnorm 27001 vielmals abschreckend und für den Mittelstand zu komplex. Das erforderliche Know-How ist oftmals im Unternehmen schlicht nicht vorhanden und wird durch einen externen IT-Dienstleister abgedeckt. Und schließlich scheinen die Kosten für die meist erforderliche externe Unterstützung bei der Einführung als sehr hoch.

SIND INFORMATIONSSICHERHEITS-SYSTEME IM MITTELSTAND SINNVOLL?

Der Nutzen sinnvoller und praxisnaher Informationssysteme gerade auch im Mittelstand liegt jedoch auf der Hand. Der tatsächliche Stand der Maßnahmen zum Schutz der betrieblichen Informationen wird erkannt, für die Unternehmensführung transparent und kann bewertet werden. Maßnahmen zur Informationssicherheit werden beherrschbar und planbar, Bedrohungsrisiken werden erkannt und in der Folge werden Budgets in Projekte investiert, in denen sie tatsächlich benötigt werden. Auf zukünftige Bedrohungen kann schneller reagiert werden und Wissen wird im Unternehmen und nicht nur bei Dienstleistern dokumentiert. Und „ganz nebenbei" erhöht ein Informationssystem das Vertrauen der Kunden und Mitarbeitenden, unterstützt bei Ausschreibungen und bei Auftragsvergaben. Optimalerweise werden bei der Einführung eines Informationssicherheitssystems auch Organisations- und Arbeitsprozesse im Unternehmen durchleuchtet, kritisch hinterfragt und auf den tatsächlichen Arbeitsalltag geprüft. Denn insbesondere in wachsenden Unternehmen oder Unternehmen mit häufiger wechselnden Mitarbeitenden schlummern im Bereich Prozessoptimierung meist ungeahnte Potentiale für weiteres Wachstum, effizientere Arbeitsweisen und damit letztlich auch erhöhte Mitarbeiterzufriedenheit.

PACKEN WIR'S AN!

Unsere Kanzlei begleitet bereits seit vielen Jahren Unternehmerinnen und Unternehmer bei der Einführung von Informationssystemen, in der Regel auf Basis des internationalen Sicherheitsstandards ISO 27001. Sprechen und diskutieren Sie unverbindlich mit unserem Team und lassen Sie uns ein paar Bedenken und Hindernisse aus dem Weg räumen. Und dann packen wir's gemeinsam an!

Ihre Ansprechpartnerin
Carina Meyer
Bachelor of Arts, IT-Sicherheitsbeauftragte

Was tun, wenn sich die Aufsichts-behörde meldet?

Welche Verfahren kann die Datenschutz-Aufsichtsbehörde anstreben und welche Handlungsbefugnisse stehen ihr dabei zur Verfügung? Wie kann man sich als Adressat einer Maßnahme verhalten und welche Gesichtspunkte sind bei einer Verteidigung gegen Maßnahmen zu berücksichtigen? Die nachfolgenden Erläuterungen geben einen Einblick in die Beantwortung dieser Fragen und zeigen Handlungsoptionen für eine möglicherweise erforderliche Verteidigungsstrategie auf.

ERSTKONTAKT & INFORMELLE KOMMUNIKATION

Der Erstkontakt mit der Aufsichtsbehörde kommt meist außerhalb eines formellen Verfahrens zustande, beispielsweise durch eine eigene, informelle Beratungsanfrage des für die Datenverarbeitung Verantwortlichen oder im Rahmen von breit angelegten Routineprüfungen der Aufsichtsbehörden. Letztere haben sich in den letzten Jahren unter anderem zu den Themenbereichen der Auftragsverarbeitungen, der Datenschutzinformationen auf Webseiten und zum Einsatz von Videoüberwachungen gehäuft.

AUFSICHTSVERFAHREN

Kommt die Aufsichtsbehörde in ihrer weiteren Prüfung der informellen Anfrage oder nach Auswertung ihrer Informationsanfrage zu dem Ergebnis, dass die durch den Verantwortlichen vorgenommene Verarbeitung datenschutzrechtlichen Vorgaben widerspricht, so stehen der Aufsichtsbehörde die in Art. 58 Abs. 1 bis 3 DSGVO normierten Untersuchungs-, Abhilfe-, Genehmigungs- und Beratungsbefugnisse zur Verfügung. Hierauf gestützt kann die Aufsichtsbehörde im nächsten Schritt mittels Verwaltungsakt dem Verantwortlichen die weitere Datenverarbeitung verbieten.

BUSSGELDVERFAHREN

Kommt der Adressat einer Anordnung der Aufsichtsbehörde dieser nicht nach oder erlangt die Aufsichtsbehörde Kenntnis von einem weiteren Verstoß gegen datenschutzrechtliche Vorgaben, so kann sie im Weiteren eine Geldbuße gemäß Art. 83 Abs. 4 bis Abs. 6 DSGVO verhängen.

„Ein Aufsichtsverfahren kann sich jederzeit in ein Bußgeldverfahren weiterentwickeln."

Die Befugnisse der Aufsichtsbehörde im Rahmen des Bußgeldverfahrens finden sich gemäß §§ 41 Abs. 2 BDSG in Verbindung mit § 46 OWiG innerhalb den allgemein für Strafverfahren geltenden Vorschriften in der Strafprozessordnung.

Die Höhe des Bußgeldes kann dabei beachtliche Ausmaße von bis zu 20 Mio. Euro erreichen, da sich die Bemessung des Betrages unter anderem an dem gesamten, weltweit erzielten Jahresumsatz eines Unternehmens orientieren kann.

STRAFRECHTLICHE VERFOLGUNG

Zusätzlich zu den Maßnahmen innerhalb des Aufsichts- und Bußgeldverfahrens ist die Einleitung eines strafrechtlichen Verfahrens möglich. Dabei sind insbesondere die, auf unrechtmäßige Datenverarbeitungen abzielenden, Strafvorschriften des § 42 BDSG und der §§ 202a, b und d StGB zu beachten.

Demnach kann beispielsweise derjenige bestraft werden, der sich unbefugt Zugang zu Daten verschafft, die nicht für ihn bestimmt sind und die gegen unberechtigten Zugang besonders gesichert wurden. Gegen einen unberechtigten Zugang besonders gesicherte Daten liegen dabei bereits dann vor, wenn ein Email Postfach mit einem geheimen, d.h. nicht öffentlichen, Passwort gegen einen unberechtigten Login geschützt wird.

HANDLUNGSOPTIONEN

Erster Schritt – Risiken abwägen

Im Rahmen einer möglichen Verteidigung gegen eine Maßnahme der Aufsichtsbehörde ist stets eine Risikoabwägung dahingehend anzustellen, welche rechtlichen, wirtschaftlichen und ideellen Folgen eine Verteidigung haben kann und welche Ziele damit erreicht werden können und sollen.

Bei einer Verteidigung im Aufsichtsverfahren ist zu beden-

„An ein Bußgeldverfahren kann sich auch eine strafrechtliche Verfolgung und Ahndung anschließen.“

ken, dass sich das Aufsichtsverfahren jederzeit in ein Bußgeldverfahren weiter entwickeln kann. Dies hat zur Folge, dass bereits bei der Wahl der Verteidigungsstrategie im Aufsichtsverfahren die Auswirkungen auf ein möglicherweise nachfolgendes Bußgeldverfahren bedacht werden müssen. Hier kann unter Umständen ein Spannungsverhältnis entstehen zwischen einer im Aufsichtsverfahren zunächst erfolgten Zusammenarbeit mit der Aufsichtsbehörde und möglicherweise kritiklosen Umsetzung der geforderten Maßnahmen auf der einen Seite, und einer Verteidigung im Bußgeldverfahren gegen die Festsetzung eines Bußgeldes auf der anderen Seite.

Die strafrechtliche Verfolgung eines datenschutzrechtlichen Sachverhalts darf ebenso nie außer Acht gelassen werden, da sich an ein Bußgeldverfahren grundsätzlich auch eine strafrechtliche Verfolgung und Ahndung anschließen kann.

Um die Chancen und Risiken im Einzelfall umfassend beurteilen zu können, sollte in diesen Fällen stets ein im Datenschutzrecht spezialisierter Rechtsanwalt (zumindest für eine Ersteinschätzung) hinzugezogen werden.

Zweiter Schritt – gezielt reagieren

Die jeweils vorhandenen Verteidigungsmöglichkeiten sind nach dieser Risikoeinschätzung je nach Verfahrensart und Verfahrensstand auszuwählen. Dabei kann beispielsweise gegen Verwaltungsmaßnahmen Rechtsschutz auf dem Verwaltungsrechtsweg erlangt werden (Widerspruch, Klage) oder im Bußgeldverfahren der Bußgeldbescheid mittels Einspruchs angegriffen werden.

FAZIT

Bereits dieser kurze Überblick macht deutlich, dass eine Vielzahl an Verteidigungsmöglichkeiten gegen Maßnahmen der Aufsichtsbehörde existieren. Und auch wenn es häufig verlockend sein mag, die von den Aufsichtsbehörden geforderten Maßnahmen kritiklos umzusetzen, kann es sich doch oftmals lohnen, in einen Dialog oder möglicherweise auch in eine rechtliche Verteidigung einzutreten.

Bei der Wahl und Durchsetzung der sinnvollsten Strategie kann ein auf das IT- und Datenschutzrecht spezialisierter Rechtsanwalt behilflich sein kann. Treten Sie in diesen Fällen gerne jederzeit mit uns in Kontakt und nutzen Sie unsere Erfahrungen und Kontakte, wenn sich, wie im Titel dieses Textes beschrieben „die Aufsichtsbehörde bei Ihnen meldet“.

Ihre Ansprechpartnerin

Chiara Bidmon
Rechtsanwältin