Newsletter

Sommer, Sonne, Ferienzeit…

Liebe Kunden und Geschäftspartner,

in fast allen Bundesländern sind oder waren inzwischen Sommerferien. So richtig sorgenfrei genießen lässt sich diese schöne Zeit und der wohlverdiente Urlaub eigentlich immer erst, wenn auch zuhause alles gut geregelt ist. Wie schön zu wissen, dass sich jemand zuverlässig um alles kümmert.

Um Ihre personellen oder fachlichen Engpässe kümmern wir uns gewohnt zuverlässig. Auch im Datenschutz sind uns inzwischen, aufgrund von Kapazitätsausweitungen, wieder kurzfristige Terminvergaben für komplexe Themen oder auch Einzelaufgaben möglich. Details hierzu finden Sie im Beitrag unseres erfahrenen Fachbereichsleiters im Bereich Datenschutz, Daniel Nyhof, der uns zudem einen Einblick in die neuesten Entwicklungen bei der europäischen Datenschutzaufsicht gewährt.

Weiterhin möchten wir Sie in diesem Newsletter bezüglich unserer Dienstleistungsqualität auf dem Laufenden halten, sowie Ihnen die Fortsetzung unserer Reihe zur modernen Internen Revision, diesmal geht es um die GIAS/Topical Requirements, ans Herz legen.

Weitere Themen in diesem Newsletter für Sie:

- ETL consit auf dem Karrieretag der IHK Lübeck
- Seminare im Fokus: Unsere neuen Seminarthemen
- EZB befasst sich mit der Auslagerung von Cloud-Diensten durch Banken
- 8. MaRisk-Novelle
- Meldestelle gemäß HinSchG: Tolles Feedback zufriedener Kunden!

Wir wünschen Ihnen einen wunderschönen Sommer!

Herzlichst

Bernd Schmid Oliver Gose

Auch im Datenschutz wieder kurzfristige Terminvergaben möglich

Gerade in Ferienzeiten kann es schnell einmal zu personellen oder fachlichen Engpässen, z.B. im Bereich des Datenschutzes kommen. Kurzfristige Lösungen gestalten sich inzwischen schnell mal als schwierig.

Aufgrund von Kapazitätsausweitungen ist es uns nunmehr wieder möglich, Sie auch im Datenschutz sehr kurzfristig und schnell in gewohnt kompetenter und pragmatischer Weise zu unterstützen.

Die Palette reicht da von temporären Aufgaben aufgrund von Abwesenheiten, z.B. als Sparringspartner von Stellvertretern, Berater von Koordinatoren, über Einzelaufgaben (z. B. Vertragsprüfungen, Dienstleisterkontrollen) als auch Gesamt-, Teil- oder Prozessaudits im Bereich des Datenschutzes. Schwerpunkte der vergangenen Zeit waren hierbei insbesondere Compliance-Prozesse, Personalmanagement, das Verzeichnis der Verarbeitungstätigkeiten (VVT) und Datenschutzfolgenabschätzungen (DSFA) sowie Datenschutzkontrollen vor Ort / in Filialen.

Sollten Sie mit Blick auf die Planung des Restjahres feststellen, dass noch Kapazitätsengpässe z. B. bei Kontrollhandlungen oder Datenschutzaudits bestehen, können wir auch hier für das dritte, und aufgrund des Vorlaufs derzeit auch noch für das vierte Quartal Kapazitäten zur Unterstützung bereitstellen.

Kommen Sie gerne auf uns zu, um sich hier entsprechende Ressourcen zu sichern.

Erneut hohe Bußgelder gegen Banken ausgesprochen...

Europas Datenschutzaufsichtsbehörden sind im Bankensektor nicht untätig geblieben und haben in den vergangenen Monaten nennenswerte Bußgelder verhängt. Hierbei stach erneut die spanische Datenschutz-aufsicht hervor, die in zwei Fällen infolge Beschwerden einzelner Personen hohe Bußgelder ausgesprochen hat.

Fehlende technisch-organisatorische Maßnahmen:
Die spanische Datenschutzbehörde reagierte im November 2023 auf die Beschwerde einer Privatperson, welche Kundin bei der beschuldigten Bank war.

Die Kundin hatte ihre Handtasche verloren, in der sich auch ihre Bankkarte befand. Die Person beantragte daher bei Ihrer Bank die Sperrung sämtlicher Bankprodukte. Dem kam die Bank jedoch nicht nach, weshalb es Dritten möglich war, unter falschen Identitäten auf die Bankprodukte der Person zuzugreifen und Geld zu überweisen. Während ihrer Untersuchung stellte die Datenschutzbehörde fest, dass der Verantwortliche es versäumt hatte, geeignete technische und organisatorische Maßnahmen (Art. 32 DSGVO) zu ergreifen, um einen solchen Fall zu verhindern und personenbezogene Daten zu schützen.

Als Sanktion wurde ein Bußgeld in Höhe von 800.000 EUR gegen die Bank ausgesprochen.

Was kann man daraus ableiten? Handlungsempfehlung für Sie:

- Achten Sie auf die Vollständigkeit Ihrer technisch-organisatorischen Maßnahmen nach Art. 32 DSGVO!
- Überprüfen Sie regelmäßig die Einhaltung und Umsetzung durch Ihre Mitarbeitenden!

Abfrage von personenbezogenen Daten:
Die spanische Datenschutzbehörde reagierte am 17.04.2024 auf die Beschwerde einer Privatperson.

Diese hatte sich beschwert, dass die Bank von ihr eine Reihe von Daten angefordert hatte. Dafür war ihr ein Dokument zum Unterschreiben übermittelt worden, in dem ihre personenbezogenen Daten bereits vorausgefüllt waren. Außerdem enthielt das Dokument eine Klausel, nach welcher sich die antragstellende Person bereiterklärte, dass die Bank ihre Daten bei der Sozialversicherungskasse anforderte. Eine Möglichkeit, dies abzulehnen, gab es nicht.

Nachdem die Person sich bei der Bank beschwert hatte und deutlich machte, dass er der Datenverarbeitungspraxis nicht zustimmte, drohte diese mit einer Sperre des Bankkontos.

Das ursprüngliche Bußgeld in Höhe von 2.000.000 EUR wurde aufgrund von Schuldeingeständnis und freiwilliger Zahlung jeweils um 20 % auf 1.200.000 EUR reduziert.

Was kann man daraus ableiten? Handlungsempfehlung für Sie:

- Achten Sie bei der Erstellung von Dokumenten darauf, dass die abgefragten personenbezogenen Daten zweckgebunden sind und eine entsprechende Rechtsgrundlage vorliegt!
- Achten Sie darauf, dass in den Dokumenten grundsätzlich der Hinweis zum Widerspruch enthalten ist!

Gerne sind wir behilflich, Ihre Datenschutzorganisation, Prozesse und Dokumente zu überprüfen, um Risiken zu erkennen und abzustellen oder zu minimieren.

Kommen Sie gerne auf uns zu – auch für ein vertrauliches und unverbindliches Erstgespräch!

Dienstleistungsqualität der ETL consit GmbH

Die ETL consit stellt an ihre Dienstleistungsqualität höchste Ansprüche. Umfassende Maßnahmen zur Sicherstellung der Qualität der erbrachten Leistungen werden in Abhängigkeit der beauftragten Dienstleistung zielgerichtet eingesetzt. Die Themen Prozess- und Qualitätsmanagement wurden hierfür eigens im Bereich Corporate Governance gebündelt.

Ein jährlicher Qualitätsbericht informiert über die Entwicklung der ETL consit und die Qualität ihrer erbrachten Leistungen als Dienstleister. Mit diesen Informationen wird die vertrauensvolle Zusammenarbeit mit unseren Mandanten unterstrichen und über die ordnungsgemäße Erfüllung der übernommenen Aufgaben und die Einhaltung der eingegangenen Verpflichtungen berichtet. Ergänzend erhalten unsere Mandanten einen Quartalsbericht mit Informationen zu ggf. aufgetretenen Datenpannen und Sicherheitsvorfällen sowie Veränderungen am Gesamtrisikoprofil.

Vor dem Hintergrund der zunehmenden Regulierung von Auslagerungsservices hat die ETL consit im Jahr 2024 ihr dienstleistungsbezogenes Internes Kontrollsystem (IKS) auf Basis des Prüfungsstandards 982 des Instituts der Wirtschaftsprüfer (IDW PS 982) zertifizieren lassen. Als Basis hierfür wurde eine IKS-Beschreibung erstellt sowie ausgewählte Kontrollaktivitäten (insbesondere für Dienstleistungsprozesse) definiert. Der Bericht des beauftragten Wirtschaftsprüfers zur Prüfung des IKS für die Dienstleistung „Interne Revision“ nach IDW PS 982 steht nunmehr mit einem positiven Prüfungsergebnis zur Verfügung.

Im Ergebnis

- sind die implementierten Grundsätze, Verfahren und Maßnahmen des IKS in der IKS-Beschreibung in Übereinstimmung mit den angewandten IKS-Grundsätzen des IPPF in allen wesentlichen Belangen **angemessen** dargestellt,
- waren die in der IKS-Beschreibung dargestellten Regelungen in Übereinstimmung mit den angewandten IKS-Grundsätzen des IPPF in allen wesentlichen Belangen

- **geeignet**, mit hinreichender Sicherheit die IKS-Ziele in Bezug auf die Dienstleistung „Interne Revision“ zu erreichen und
- **wirksam**.

Mit dieser externen „Zertifizierung“ sehen wir unsere hohen Qualitätsziele auch durch einen unabhängigen Wirtschaftsprüfer bestätigt.

Sollten Sie Interesse an den Prüfungsergebnissen zu unserem IKS haben, sprechen Sie uns gerne an.

EZB befasst sich mit der Auslagerung von Cloud-Diensten durch Banken

Die Europäische Zentralbank (EZB) hatte ein Konsultationsverfahren zur Auslagerung von Cloud-Diensten an Cloud-Anbieter eingeleitet.
Banken und andere mit der Auslagerung von Cloud-Diensten befasste Parteien waren eingeladen, ihre Kommentare einzureichen.

Der Leitfaden, der im Rahmen dieses Verfahrens erstellt wird, erläutert aufsichtliche Erwartungen und Best Practices für die Auslagerung von Cloud-Diensten durch Banken. Ziel ist es, Klarheit über die diesbezüglichen rechtlichen Anforderungen zu schaffen und einheitliche Wettbewerbsbedingungen zu schaffen. Der Leitfaden konzentriert sich insbesondere auf prozessuale Schwachstellen und bewährte Verfahren, die bei der laufenden Aufsicht identifiziert wurden. Banken nutzen zunehmend Cloud-Computing-Dienste von Drittanbietern, die zwar potenziell preiswerter, flexibler und sicherer sind, aber auch Abhängigkeiten und Risiken mit sich bringen. Die EZB empfiehlt, diese Risiken explizit im Risikomanagement zu berücksichtigen.

Im Rahmen ihrer Überprüfungen stellte die EZB Schwachstellen in den IT-Auslagerungsvereinbarungen der Banken fest, weshalb das Management von Drittparteirisiken, einschließlich Cloud-Outsourcing, weiterhin zu den Hauptaufsichtsprioritäten der EZB gehört.

Die EU-Gesetzgeber haben den Digital Operational Resilience Act (DORA) verabschiedet, um das IKT-Risikomanagement zu verbessern. Dieser verpflichtet Banken, Risiken im Zusammenhang mit Auslagerungen proaktiv zu mindern und Rahmenwerke für IT-Sicherheit und Cyberresilienz zu erstellen. Das öffentliche Konsultationsverfahren lief bis zum 15. Juli 2024, nunmehr werden die eingegangenen Kommentare ausgewertet und der endgültige Leitfaden erstellt.

Topical Requirements ergänzen die Global Internal Audit Standards

Das Institutes of Internal Auditors (IIA) hat am 09.01.2024 die Global Internal Audit Standards (GIAS) veröffentlicht. Die GIAS sind eine global anerkannte betriebswirtschaftliche Norm und so für alle Internen Revisionen verbindlich. 52 Standards in fünf Domains regeln die Prinzipien und Anforderungen zur Sicherung

der Qualität der Internen Revision und geben Richtlinien zur erfolgreichen Umsetzung.
Diese Standards sollen um spezifische Anforderungen zu (derzeit) acht aktuellen Risikothemen ergänzt werden:

1. Cybersicherheit
2. Nachhaltigkeit, ESG
3. Dienstleistermanagement
4. IT-Governance
5. Beurteilung organisatorischer Governance
6. Fraud-Risikomanagement
7. Datenschutz-Risikomanagement
8. Öffentlicher Sektor: Wirkungsprüfungen

Ausgenommen zum Thema „Cybersicherheit“ (aktuell in Konsultation) liegen die Texte zu diesen sog. Topical Requirements zur Mitte des Jahres 2024 noch nicht vor.
Die Topical Requirements sollen eine Struktur für häufig geprüfte Themen bieten, die typischerweise ein höheres Risiko darstellen und von Natur aus weit verbreitet sind. Während die Standards für alle Revisionsleistungen gelten, sind die Topical Requirements als zusätzliche Anforderungen zu betrachten, die verbindlich zu befolgen sind, wenn das Thema im Fokus eines Auftrags der Internen Revision steht.

Die Anwendung der Topical Requirements soll die Professionalität des Berufsstands der Internen Revision für die sich entwickelnde globale Risikolandschaft stärken und den Wert der Revisionsleistungen branchen- und sektorenübergreifend erhöhen. Die Einhaltung der Topical Requirements soll den Internen Revisorinnen und Revisoren helfen, die Qualität und Konsistenz ihrer Aufträge zu erhöhen.

Die Topical Requirements sind so strukturiert, dass sie eine konsistente Prüfungsmethodik für die Erbringung von Revisionsleistungen in den Bereichen Governance-, Risikomanagement- und Kontrollprozesse enthalten. Jeder Bereich umfasst:

- Anforderungen, die verbindlich sind und wesentliche organisatorische Ziele abdecken.
- Überlegungen, die nicht verbindlich sind, sondern als Best Practices für die Bewertung der Gestaltung und Umsetzung der organisatorischen Ziele dienen.

Die Einhaltung der Topical Requirements wird künftig auch bei externen Quality Assessments bewertet. Informieren Sie sich frühzeitig über die Anforderungen zu den jeweiligen Themen und dokumentieren Sie deren Umsetzung. Wir unterstützen Sie gerne und freuen uns über einen fachlichen Austausch.

ETL consit auf dem Karrieretag der IHK Lübeck!

Am Mittwoch, den 29. Mai 2024, durfte sich die ETL consit GmbH als Arbeitgeber auf dem Karrieretag der IHK zu Lübeck vorstellen. Auf dem „Hanse Innovation Campus“ konnten Jana Zickermann-Bülow, Daniel Nyhof und Joshua Witt den Studierenden und Absolventen der Universität zu Lübeck und der Technischen Hochschule Lübeck sowohl unser Unternehmen als auch konkrete Jobangebote (u. a. als Junior-Berater für Informationssicherheit und IT-Revisor) präsentieren.

Dabei wurden viele gute Gespräche geführt und wir sind zuversichtlich, in naher Zukunft dann auch von Zuwachs im Team der ETL consit berichten zu können!

Die ETL consit wird in diesem Jahr auch an weiteren Messen für den akademischen Nachwuchs (u. a. in Hamburg (17.10.2024) und Kiel (13.11.2024)) teilnehmen, und freut sich darauf, auch hier in Kontakt mit vielen interessierten Berufseinsteigern treten zu können. Gerne bieten wir die Chance auf einen gelungenen Berufsstart in einem dynamischen Beratungsumfeld und mit spannenden Zukunftsthemen (AI, Cybersecurity, Digitalisierung…), sowie Chancen und Karrierewege, und die vielfältigen Möglichkeiten der ETL-Gruppe (berufsbegleitendes Master-Studium, Fortbildungsmöglichkeiten…).

Aktuelle Stellenangebote der ETL consit GmbH

Seminare im aktuellen Fokus: Die ETL-Akademie empfiehlt…

8. MaRisk-Novelle	Nächster Termin:26.08.2024	Jetzt anmelden
Fachkundeschulung gem. § 15 Abs. 2 HinSchG für MA von Banken	Nächster Termin:03.09.2024	Jetzt anmelden
DORA für Revisoren	Nächster Termin:03.09.2024	Jetzt anmelden

Unser Gesamtprogramm

8. MaRisk-Novelle veröffentlicht !

Am 29.05.2024 hat die BaFin die 8. Novelle ihrer MaRisk veröffentlicht.

Die Neuerungen, die sich im Wesentlichen im Bereich der Zinsänderungs- und Kreditspreadrisiken im Anlagebuch erschöpfen, sind zwar zunächst überschaubar, erfordern jedoch eine intensive Prüfung der Prozesse. Die BaFin setzt dabei auf eine zweigliedrige Regelungsstruktur, die sowohl handelsrechtliche als auch ökonomische Perspektiven berücksichtigt. Punktuelle Ergänzungen und Verweise auf die EBA-Leitlinien spielen eine wichtige Rolle.

Im Zusammenhang mit den Zinsänderungsrisiken wird sowohl die handelsrechtliche wie auch die ökonomische Perspektive bezüglich mehrerer Dimensionen gefordert: Bezüglich der Entscheidung über die Risikoneigung, der Risikosteuerung und der Bewertung der Auswirkungen (Auswirkungen auf die GuV einerseits und auf den Barwert der jeweiligen Positionen andererseits). Im Hinblick auf die Risikosteuerung werden dabei Details vorgegeben, wie z.B. eine genaue Definition von Messgrößen, die Beschreibung des Charakters des sog. Zinsschocks (also einer Änderung der Zinskurve) nach Art und Umfang oder den Verfahren zur Modellierung des Cashflows.

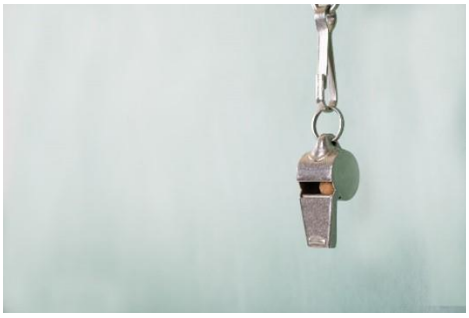
Kreditspreadrisiken sind als eine neue Kategorie wesentlicher Risiken aufgenommen. Auch hier ist nun die Betrachtung sowohl der handelsrechtlichen als auch der ökonomische Perspektive notwendig, wie bei den Zinsänderungsrisiken. In einem ersten Schritt müssen unter sämtlichen Positionen des Anlagebuches jene identifiziert werden, die einem Kreditspreadrisiko unterliegen, wobei für alle Positionen, die dabei nicht berücksichtigt werden, zu begründen ist, weshalb dies so entschieden wurde. Darüber hinaus sind weitere Vorgaben der EBA-Leitlinien zur Identifizierung von Risiken zu berücksichtigen.

Die Regelungen der EBA-Leitlinien sind des Weiteren auch für Stresstests zu beachten, sowie für das Berichtswesen.

Die ETL consit macht Sie gern mit allen Neuerungen vertraut.

Meldestelle gemäß Hinweisgeberschutzgesetz: Tolles Feedback zufriedener Kunden!

Unter unseren ersten Kunden, für die wir als Meldestelle gemäß HinSchG fungieren, befinden sich u.a. eine mittelgroße Wirtschaftsprüfungsgesellschaft und ein Unternehmen, welches auf dem Gebiet der gewerblichen und industriellen Befestigungstechnik weltweit zu den Führenden seiner Branche gehört.



Wir freuen uns sehr über das ausgesprochen gute Feedback aller unserer Kunden.

Da das Hinweisgeberschutzgesetz noch sehr jung ist, bestand der erste Unterstützungsbedarf seitens unserer Kunden naturgemäß darin, ihnen bei der Einrichtung des Hinweisgebersystems zur Seite zu stehen. Dies umfasste die Beratung, wie sie die vorgeschriebenen vertraulichen Meldekanäle am besten einrichten, so dass Hinweisgeber verlässlich und vertraulich unsere Meldestellen-Mitarbeiter erreichen können, und auch, dass diese sich mit Verantwortlichen im Kundenunternehmen streng vertraulich über mögliche Folgemaßnahmen abzustimmen in der Lage sind. Anforderungen anderer Rechtsgrundlagen, z.B. die Beschwerdestelle gegen Diskriminierungen am Arbeitsplatz (gemäß § 13 des Allgemeinen Gleichbehandlungsgesetzes AGG) konnten optional synergetisch einbezogen werden.

Darüber hinaus halfen wir bei der Veröffentlichung der Informationen zu den Meldekanälen.

Außerdem schulen wir Mitarbeiter von Unternehmen, die die Meldestelle im eigenen Haus betreiben wollen, im Rahmen einer ganztägigen Fachkundeschulung, die auch zahlreiche praktische Übungen in Kleingruppen enthält, so dass sie im Anschluss die notwendigen Kenntnisse besitzen, um die Aufgaben der Meldestelle übernehmen zu dürfen. Auch diesbezüglich waren wir über das ausgesprochen gute Feedback der Teilnehmenden sehr erfreut.

Unterstützung zur Umsetzung HinSchG

Immer eine gute Idee…sprechen Sie uns gerne an!

Ihre Ansprechpartner

Bernd Schmid
Geschäftsführer
Telefon (04531)6696-28
Mobil (0160)90175068
bernd.schmid@etl-consit.de

Oliver Gose
Mitglied der Geschäftsführung
Telefon (04531)66 96-422
Mobil (0162) 372 42 17
oliver.gose@etl-consit.de

ETL consit GmbH
Schützenstraße 25a
23843 Bad Oldesloe
Telefon (04531) 66 96-0
Fax (04531) 66 96-45
info@etl-consit.de
www.etl-consit.de