Dr. Johannes Neumayer:
Ein Gespenst namens DORA… … und eine Anregung, die Zeit zu nutzen.

Ein Gespenst namens Dora (Verordnung (EU 2022 /2554 **D**igital **O**perational **R**esilience **A**ct) und eine Anregung, die Zeit zu nutzen, ohne Anspruch auf umfassende Darstellung der umfangreichen Reglungen!

Was ist neu gegenüber den bekannten Pflichten nach der DSGVO?
Darüber berichtet heute Dr. Johannes Neumayer unten anbei.

Die **bisher erschienen Praxis-Beiträge auszugsweise:**

DSGVO 22: **Ausweiskopien** in der täglichen Praxis. Hier…
DSGVO 21: Ein Gespenst namens **DORA.** Hier…
DSGVO 20: Vorsicht bei **Software**. Hier…
DSGVO 19: EuGH zu Schadenersatz nach Hacker-Angriff. Nutzen Sie TOMs, um sich freizubeweisen. Hier...
DSGVO 18: Wann ist eine **Datenpanne** zu **melden?** Hohe Strafen drohen! Hier...
DSGVO 17: **EU-USA Datenschutz-Abkommen:** Sind Google & Co nun wieder erlaubt? Hier...
DSGVO 16: USA wollen **TikTok** verbieten. Hier...
DSGVO 15: Praxisfragen zu **Kommunikationstools.** Hier...
DSGVO 14: Urteil droht **250.000 €** wegen **Google Fonts** an. Hier…

IDD 16: Alles in **GISA** eingetragen? **Konsequenzen?** Hier...
IDD 15: Seit 1.5. **Altersdiskriminierung** verboten. Oder doch nicht? Hier...
IDD 14: **Aufbewahrung Beratungs- und Verkaufsunterlagen:** Was sagen IDD / DSGVO dazu? Hier...
IDD 13: IDD **Aufsicht: Grobe Mängel aufgedeckt.** Welche Behörde kontrolliert bei Ihnen was? Hier...
IDD 12: Die neue Whistleblower-Richtlinie. Was müssen Sie tun? Hier...
IDD 11: Die **Behörde kommt.** Wie darauf **vorbereiten?** Hier...
IDD 10: Wann und wie darf man **Kunden und Interessenten noch kontaktieren?** TKG? Hier...

Praxis 4: **Erlagschein-Gebühr** schon wieder. Was sagt **OGH** dazu? Hier...
Praxis 3: Wie setzt man neue Whistleblowing-Vorgaben (Einrichtung Meldesystem, etc.) um? Hier...
Praxis 2: Aktuelle **EDV-Gefahren**, typische **Einfallstore** und Betrugsmaschen. Hier…
Praxis 1: Praxis von **Abmahnanwälten** kann teuer werden. Hier…

ALLE bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen…
Oder kostenlos mit "JA zu INFO" an g.wagner@b2b-projekte.at anfordern.

Unten folgt nun der Beitrag, den uns Dr. Neumayer zur Verfügung gestellt hat.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

Dr. Johannes Neumayer: Ein Gespenst namens DORA…
… und eine Anregung, die Zeit zu nutzen.

Ein Gespenst namens Dora (Verordnung (EU 2022 /2554 **D**igital **O**perational **R**esilience **A**ct) und eine Anregung, die Zeit zu nutzen, ohne Anspruch auf umfassende Darstellung der umfangreichen Reglungen!

Den Glauben, dass in Wahljahren keine einschneidend drakonischen Gesetze erlassen würden, haben das Europäische Parlament und der Rat der EU mit der DORA-Verordnung und der begleitenden Richtlinie nachhaltig widerlegt und nicht bloß im Nebengewerbe tätigen Versicherungsvermittlern und Wertpapierfirmen erneut erheblichen Organisationsaufwand nicht nur im IT-Bereich aufgebürdet, womit endgültig **das Opfer von Cyberangriffen kriminalisiert** und dem Versicherungs- und Finanzbereich eine Organisationspflicht der Herbeiführung technisch hoher Resilienz gegen Angriffe gegen dessen Informations- und Kommunikationstechnologien (richtig „Systeme“) im Akronymrausch des EU Gesetzgebers **IKT** genannt, aufgebürdet wurde, leider vergleichbar einer Norm, die alten oder schwachen Personen bei sonstiger Strafe die Pflicht aufbürden würde, durch Selbstverteidigungskurse (“**Cyberhygiene**“) oder Bewaffnung oder ausreichend viele Bodyguards jeden Überfall („**IKT Risiko“**) in schlecht beleuchteten Hinterhöfen zu unterbinden.

Was ist neu gegenüber den bekannten Pflichten nach der DSGVO?

1.Die Pflichten sind in Art 17 leicht entschärft für kleine nicht verflochtene Wertpapierfirmen und durch den Grundsatz der Verhältnismäßigkeit (Art 4).

2. Hauptpflicht (Art 5) ist die Erstellung eines **Governance- und Kontrollrahmens**, der ein wirksames Management und ein hohes Niveau digitaler Resilienz erreichen soll, die **dem Leitungsorgan zur persönlichen Plicht** gemacht wird, was Delegierungen an besondere Verantwortliche (§ 9 VStG) massiv erschweren dürfte.

So sind explizit **Leitlinien** zu erstellen und klare V**erantwortungsbereiche** aller IKT-Funktionen zu definieren und eine **Resilienzstrategie** inkl. **IKT-Reaktions- und Wiederherstellungspläne** zu entwickeln und die Umsetzung und Tauglichkeit der Maßnahmen laufend zu überprüfen und zu testen.
3. Nach Art 19 sind **schwerwiegende Vorfälle,** die somit umfassende **nachteilige Auswirkungen** auf das Netzwerk bzw. Informationssystem oder die Funktionen des Unternehmens haben (Art 4 Z10) der Aufsichtsbehörde zu melden und auch **potentiell betroffene Kunden** über mögliche Schutzmaßnahmen zu informieren.

4. Die Plichten können an geeignete Dienstleister ausgelagert werden.

5. Nach Art 24 haben die betroffenen Unternehmen ihr System zu testen, nach Art 13 ihr Personal zu schulen und die Systeme laufend zu verbessern. Leitende Angestellte haben einmal jährlich dem Leitungsorgan über Vorfälle zu berichten.

6. Nach Art 14 sind **Kommunikationspläne über Vorfälle zu erstellen,** dies unter Trennung der Mitarbeiter des Risikomanagements und der Schadensbeseitigung (Wiederherstellung).

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

7. **Ausgenommen** von den Kernpflichten nach Art 5 bis 15 sind kleine und nicht verflochtene Wertpapierfirmen, die dennoch einen „soliden“ Risikomanagementrahmen zu entwickeln und zu installieren und **wesentliche Abhängigkeiten von IKT-Dienstleistern zu identifizieren und Tests durchzuführen** und die Schulungen des Personals zu organisieren haben.

8. Die **Anweisungen** im Rahmen des IKT-Risikomanagementrahmens **sind zu dokumentieren** und auf Anfrage der Behörde ein Bericht vorzulegen.

9. Das **Erfordernis zur Verringerung des Drittparteienrisikos** zwingt zur sorgfältigen Auswahl der EDV-Dienstleiter und Cloud-Provider. Die Behörden können IKT-Dienstleister als kritisch einstufen und damit de facto vom Markt ausschließen (Art 31).

10. Die Behörden können sogar Gebühren für die Überwachung verlangen.

Folgerungen:

1. **Auch Kleinunternehmen haben einen soliden und dokumentierten IKT-Risikomanagementrahmen zu errichten** und aufrechtzuerhalten, in dem die Mechanismen und Maßnahmen für ein rasches, effizientes und umfassendes Management des IKT-Risikos, einschließlich des Schutzes der einschlägigen physischen Komponenten und Infrastrukturen, detailliert sind:

a) die Sicherheit und das Funktionieren aller IKT-Systeme fortlaufend zu überwachen.

b) die **Auswirkungen von IKT-Risiken zu minimieren,** indem solide, resiliente und aktualisierte IKT-Systeme, -Protokolle und -Tools, die zur Unterstützung der Durchführung ihrer Tätigkeiten und zur Bereitstellung von Diensten angemessen sind, verwendet werden, und in angemessener Weise die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten in den Netzwerk- und Informationssystemen zu schützen; die wesentlichen Abhängigkeiten von IKT-Drittdienstleistern zu ermitteln; eine rasche Ermittlung und Aufdeckung der Ursachen von IKT-Risiken und -Anomalien in den Netzwerk- und Informationssystemen sowie eine rasche Handhabung von IKT-Vorfällen zu ermöglichen, die Kontinuität kritischer oder wichtiger Funktionen durch Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die zumindest Sicherungs- und Wiedergewinnungsmaßnahmen umfassen, zu gewährleisten.

c) eine **rasche Ermittlung und Aufdeckung der Ursachen von IKT-Risiken und -Anomalien** in den Netzwerk- und Informationssystemen sowie eine rasche Handhabung von IKT-Vorfällen ermöglichen;

d) die **wesentlichen Abhängigkeiten von IKT-Drittdienstleistern** ermitteln;

e) die **Kontinuität kritischer oder wichtiger Funktionen** durch Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die zumindest Sicherungs- und Wiedergewinnungsmaßnahmen umfassen, gewährleisten;

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at

f) die Pläne und Maßnahmen sowie die **Wirksamkeit der durchgeführten Kontrollen regelmäßig zu testen;** und in den IKT-Risikobewertungsprozess einzubeziehen und entsprechend dem Bedarf und dem IKT-Risikoprofil Programme zur Sensibilisierung für IKT-Sicherheit sowie **Schulungen zur digitalen operationalen Resilienz für Personal und Management zu entwickeln;** bei Verträgen mit Dienstleistern sind die Standardvertragsklauseln der ESA zu implementieren oder als Hilfskrücke diese als zukünftige Vertragsbestandteil zu vereinbaren.

2. **An der internen Analyse der IKT-Gefahren** führt kein Weg vorbei, wohl auch nicht an professioneller Hilfe zur Erstellung des IKT-Risikomanagementrahmens, sei es von der Kammerorganisation und den Experten des Vertragspartnerversicherers.
Die **Datenwiederherstellung ist schon im Eigeninteresse zu gewährleisten**, sei es durch eine extra Festplatte im Safe. Die **Vorbereitung eines Berichts an die Aufsichtsbehörde** (die einen solchen abverlangen kann und wohl auch wird) über die gesetzten Maßnahmen und internen Richtlinien ist ratsam.

Nach den Sicherheitsberichten vieler Behörden geht die **größte Gefahr von halbstaatlichen Hackern aus Ländern hervor,** die direkt oder indirekt in den Ukrainekrieg involviert sind, sodass die häufige Auschlussklausel für Schäden aus kriegerischen Ereignissen und Terrorismus in vielen Haftplichtversicherungsverträgen („Nicht versichert sind Ansprüche wegen Schäden, die u. a. auf Kriegsereignissen, inneren Unruhen, Terrorakten oder Generalstreik beruhen“) greifen könnte.

Hilfreich neben der Mitteilung des Fachverbandes Finanzdienstleister sind jene der Bafin (hier klicken...) wo auch mögliche Vertragsinhalte für beauftragte EDV-Dienstleister enthalten sind.

Typisch EU ist der legistische Overkill, eine Verordnung **und** eine Richtlinie mit Ausführungsgesetzgebung der Länder und zahllose Ermächtigungen der Aufsichtsbehörden, näheres und Interpretationen der unbestimmten Begriffe in der DORA Materie festzulegen, was bewirkt, dass oft so getan wird, als wäre eine neue Auslegung der Behörden, die schon immer einzig gültige und richtig, entgegen dem Gegensatz des § 5 ABGB, dass Gesetze **nicht** zurückwirken.

Ich hoffe, ich habe das Problembewusstsein geweckt und Sie werden kein „DORA-Opfer“.

Beste Grüße von Dr. J. Neumayer und Günter Wagner

ALLE bisherigen IDD und DSGVO-Praxisbeiträge können Sie hier herunterladen…
Oder kostenlos mit "JA zu INFO" an g.wagner@b2b-projekte.at anfordern.

Mag. Günter Wagner, B2B Projekte für Finanz- und Versicherungsbranche
Wurmsergasse 7, 1150 Wien, Tel: 0676-545 789 1, Fax: 01-786 84 79, g.wagner@b2b-projekte.at