BI § ET

SAP SECURITY GROUP

VIENNA EDITION

WHERE SECURITY
SHAPES THE FUTURE

Rechtliche Fallstricke im Berechtigungsmanagement

Pflichten des Unternehmens – und wann die Leitung selbst haftet

accenture | ITing quality

5. November 2026

Alte Börse | Schottenring 16 | 1010 Wien | Österreich

BI§SET

RA Mag. Katharina Bisset, MSc



- Selbstständige Rechtsanwältin (IT/IP)
- Co-Founderin NetzBeweis & Nerds of Law
- Disziplinarrätin in der RAK Niederösterreich
- Lektorin

- Rechtswissenschaften (Mag.iur.)
- Business Process Engineering & Management (MSc)
- CIPP/E
- Scrum Master PSM I, PMA Level D

OGH 19.11.2024, 4 Ob 195/24s

3,5 Monate

nach dem Ausscheiden: Eine Ex-Mitarbeiterin loggt sich ein.

Ihr Zugang war nach dem Ausscheiden nicht gesperrt worden. Deshalb scheiterte das Unternehmen mit seinem Antrag auf Beweissicherung gegen die Mitbewerberin: Es fehlten angemessene Geheimhaltungsmaßnahmen.



BI§ET

Drei Botschaften für heute

1

Unternehmenspflicht

Mehrere Gesetze verlangen ein wirksames Berechtigungs-management.

2

Aufgabe der Leitung

Sie muss organisieren und überwachen, teils ausdrücklich per Gesetz.

3

Persönliche Haftung

Bei schuldhaften Versäumnissen. Ihre Sorgfalt muss sie nachweisen können.

TEIL 1

TEIL 2



Ein Fall in drei Jahren

2024

Vertretung

Die Kreditorenbuchhalterin bekommt Stammdatenrechte. Danach bleiben sie. Sie kann jetzt Bankdaten ändern und Zahlungen freigeben.

2025

Prüfhinweis

Der Abschlussprüfer meldet den Konflikt im Management Letter an die Geschäftsführung. Behebung: „mit der S/4-Migration“.

2026

Betrug

Gefälschte Lieferanten-Mail mit neuer IBAN. Sie ändert die Bankdaten und gibt selbst frei: 480.000 € weg.

Teil 1: Hat das Unternehmen seine Pflichten erfüllt?

Teil 2: Haftet die Geschäftsführerin persönlich?

Fiktiver Praxisfall



Vier Regelwerke, ein gemeinsamer Nenner

DSGVO

personenbezogene Daten

Zugriffsschutz als Datenschutzpflicht

NISG 2026

erfasste Einrichtungen, 18 Sektoren

Zugriffskontrolle als Risiko-management

DORA

erfasste Finanzunternehmen

Feste Prüfzyklen für Zugriffsrechte

CRA

Hersteller erfasster Produkte

Zugriffsschutz als Produkt-anforderung, gestaffelt

Geschäftsgeheimnisse: Maßnahmen zum Schutz
GmbH und AG: ein dem Unternehmen angemessenes internes Kontrollsystem

Unterschiedliche Anwendungsbereiche, mehrere können gleichzeitig gelten. Orientierung, keine Betroffenheitsprüfung.



DSGVO: Zugriffsschutz ist Datenschutz

72 h

Meldung: unverzüglich, möglichst binnen 72 h, wenn ein Risiko besteht

GILT FÜR

Personenbezogene Daten im Anwendungsbereich der DSGVO

PFLICHT DES UNTERNEHMENS

Geeignete technische und organisatorische Maßnahmen, deren Wirksamkeit regelmäßig überprüft wird (Art. 24, 25, 32)

FÜR IHRE BERECHTIGUNGEN

Zugriff nach Aufgabe. Nicht mehr benötigte Rechte entziehen, etwa bei Wechsel oder Austritt.

WAS DROHT

Bis 10 Mio. € oder 2 % (Art. 32), bis 20 Mio. € oder 4 % (u. a. Art. 5), jeweils der höhere Betrag. Dazu Schadenersatz (Art. 82).

Art. 5, 24, 25, 32–34, 82, 83 DSGVO · EuGH C-340/21



DSGVO: Schutzziele nach Art. 32

Vertraulichkeit	Unberechtigten Zugriff verhindern. Beispiel: Rollen und Freigaben.
Integrität	Unerlaubte Änderungen verhindern. Beispiel: Funktionstrennung.
Verfügbarkeit	Daten nutzbar halten und wiederherstellen. Beispiel: Backup und Restore-Test.
Belastbarkeit	Systeme und Dienste dauerhaft belastbar halten.
Wirksamkeit	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Maßnahmen.

Art. 32 DSGVO · Beispiele sind Umsetzungsvorschläge, keine abschließende Maßnahmenliste



DSGVO: Berechtigungen als TOM

Zugriff nach Aufgabe	Lesen, Ändern und Exportieren als Kontrollziele unterscheiden. Eine universelle technische Trennung folgt daraus nicht.
Voreinstellungen	Datenschutzfreundliche Standardrechte und geregelte Sonderrechte (Art. 25).
Wechsel und Austritt	Nicht mehr benötigte Rechte entziehen und Rechte regelmäßig überprüfen.
Leitungsfrage	Welche Nachweise zeigen, dass die Rechte tatsächlich passen?

Art. 25 und 32 DSGVO · praktische Umsetzung



DSGVO: die Meldeentscheidung

Auslöser	Verletzung des Schutzes personenbezogener Daten. Immer intern dokumentieren (Art. 33 Abs. 5).
Kein Risiko	Voraussichtlich kein Risiko für Rechte und Freiheiten: keine Meldung an die Behörde.
Risiko	Meldung an die Datenschutzbehörde: unverzüglich, möglichst binnen 72 h ab Kenntnis.
Hohes Risiko	Meldung an die Behörde und unverzügliche Benachrichtigung der Betroffenen (Ausnahmen Art. 34 Abs. 3).
Auftragsverarbeiter	Informiert den Verantwortlichen unverzüglich. Keine eigene 72-Stunden-Frist.

Art. 33 und 34 DSGVO · Datenschutzbehörde: Data-Breach-Verfahren



DSGVO: Rechtsfolgen

Art. 83 Abs. 4	U. a. Art. 32: bis 10 Mio. € oder 2 % des weltweiten Vorjahresumsatzes, jeweils der höhere Betrag.
Art. 83 Abs. 5	U. a. Art. 5: bis 20 Mio. € oder 4 %. Greift nicht automatisch bei jedem Sicherheitsverstoß.
Art. 82	Schadenersatz bei Verstoß, ersatzfähigem Schaden und Kausalzusammenhang.
Organhaftung	Gesondert prüfen: Pflicht, Verschulden, Schaden, Kausalität. Eine Geldbuße ist nicht automatisch regressfähig.

Art. 82 und 83 DSGVO · Unternehmensfolgen und Organhaftung trennen



Geschäftsgeheimnisse brauchen Zugriffskontrolle

§ 26b

UWG: Geheimnis nur mit angemessenen Geheimhaltungs-maßnahmen

GILT FÜR

Jedes Unternehmen mit vertraulichem Know-how, z. B. Konditionen und Kalkulationen

VORAUSSETZUNG DES SCHUTZES

Angemessene Geheimhaltungsmaßnahmen treffen. Ohne sie liegt rechtlich kein Geschäftsgeheimnis vor (§ 26b Abs. 1 Z 3).

FÜR IHRE BERECHTIGUNGEN

Zugriff nur für die, die es brauchen. Zugänge beim Ausscheiden unverzüglich sperren (OGH 4 Ob 195/24s).

WAS VERLOREN GEHT

Keine Geldbuße, aber kein Schutz: Unterlassung, Schadenersatz und Beweissicherung können scheitern.

§§ 26b ff. UWG · § 26b Abs. 1 Z 3 UWG · OGH 19.11.2024, 4 Ob 195/24s



NISG 2026: Zugriffskontrolle ist Pflicht

§ 32

Risikomanagementmaßnahmen, ausdrücklich auch Zugriffskontrolle

GILT FÜR

Erfasste Einrichtungen, 18 Sektoren, meist ab mittlerer Größe
Registrierung bis31.12.2026

PFLICHT DES UNTERNEHMENS

Maßnahmen nach NISV 2026 und VO (EU) 2024/2690 umsetzen und ihre Wirksamkeit prüfen

FÜR IHRE BERECHTIGUNGEN

Need-to-know, Funktionstrennung, Drittzugänge begrenzen, geplante Überprüfung (Anh. 11.2)

WAS DROHT

Bis 10 Mio. € / 2 % (wesentlich) bzw. 7 Mio. € / 1,4 % (wichtig), jeweils der höhere Betrag (§ 45)

§§ 24–29, 32, 45 NISG 2026 · §§ 2, 4 NISV 2026 · Anh. 11.2, 11.3 VO (EU) 2024/2690



NISG 2026: Governance und NISV

§ 31 NISG	Leitungsorgane stellen die Einhaltung der Risikomanagementmaßnahmen sicher und beaufsichtigen sie. Schulungspflicht.
§ 32 NISG	Risikomanagementmaßnahmen, darunter Zugriffskontrolle und Bewertung der Wirksamkeit.
§ 2 NISV 2026	Erstreckt die Anforderungen der DurchführungsVO (EU) 2024/2690 auf weitere Einrichtungsarten.
§ 4 NISV 2026	Kompensierende Maßnahmen: begründet dokumentieren, mindestens jährlich auf Wirksamkeit prüfen.
Weitere Normen	Betroffenheit und Registrierung §§ 24–29, Nachweise § 33, Vorfälle §§ 34–35.

§§ 24–35 NISG 2026 · §§ 2, 4 NISV 2026 · VO (EU) 2024/2690



Zugriffskontrolle nach NIS2 Durchführungs-VO

Lebenszyklus	Zugriffsrechte vergeben, ändern, entziehen und dokumentieren; Genehmigung durch zuständige Personen.
Grundsätze	Need-to-know, minimale Rechte, Funktionstrennung.
Personal	Rechte bei Wechsel oder Ende der Beschäftigung anpassen.
Dritte	Besucher, Lieferanten und Dienstleister nach Umfang und Dauer beschränken.
Nachweis	Register, Protokollierung, Überprüfung in geplanten Abständen und nach Organisationsänderungen.

Anhang Punkt 11.2 DurchführungsVO (EU) 2024/2690 · privilegierte Konten: Punkt 11.3



NISG 2026: Geldstrafen und Zurechnung

Wesentliche	Bis 10 Mio. € oder 2 % des weltweiten Vorjahresumsatzes, jeweils der höhere Betrag.
Wichtige	Bis 7 Mio. € oder 1,4 %, jeweils der höhere Betrag.
§ 45 Abs. 4	Gesonderter Rahmen für bestimmte Verstöße: bis 50.000 €, im Wiederholungsfall 100.000 €.
§ 44	Zurechnung an die Einrichtung. Wurde sie bestraft, ist von der Bestrafung des Verantwortlichen nach § 9 VStG abzusehen (Abs. 5).

§§ 44, 45 NISG 2026



NISG 2026: Untersagung der Leitung

Wer	Nur wesentliche Einrichtungen (§ 39 Abs. 4).
Auslöser	Ein Bescheid nach § 39 Abs. 2 wird nicht fristgerecht und nachweislich befolgt.
Folge	Vorübergehende Untersagung der Leitungsaufgaben in dieser Einrichtung, Eintragung im Firmenbuch.
Ende	Unverzügliche Aufhebung nach nachgewiesener Erfüllung (Abs. 5).
Ausnahme	Stellen der öffentlichen Verwaltung (Abs. 6).

§ 39 NISG 2026



DORA: feste Prüfzyklen für Zugriffsrechte

6 Monate

Prüfabstand bei kritischen oder wichtigen Funktionen

GILT FÜR

Erfasste Finanzunternehmen, seit 17.1.2025; vereinfachter Rahmen gesondert

PFLICHT DES UNTERNEHMENS

IKT-Risikomanagementrahmen mit geregelter Kontrolle der Zugangs- und Zugriffsrechte (Art. 6, 9)

FÜR IHRE BERECHTIGUNGEN

Minimale Rechte, Funktionstrennung, Zurechenbarkeit, unverzüglicher Entzug. Sonst jährlich prüfen.

WAS DROHT

Aufsichtsrechtliche Maßnahmen und Sanktionen nach Finanzmarktrecht. Bezug von IKT-Diensten entlastet nicht (Art. 28).

Art. 6, 9, 16, 28 DORA · Art. 21 lit. e sublit. iv Delegierte VO (EU) 2024/1774



CRA: relevant, wenn Sie Hersteller sind

24 h

Frühwarnung ab Kenntnis, Pflicht seit 11.9.2026

GILT FÜR

Hersteller erfasster Produkte mit digitalen Elementen. Hauptpflichten ab 11.12.2027

PFLICHT DES UNTERNEHMENS

Sicherheit über den Lebenszyklus: Risikoanalyse, Schwachstellenbehandlung, Sicherheitsupdates

FÜR IHRE BERECHTIGUNGEN

Schutz vor unbefugtem Zugriff (Authentifizierung, Berechtigungen) wird Produktanforderung (Anhang I)

WAS DROHT

Mit den Hauptpflichten ab 11.12.2027: Bußgelder bis 15 Mio. € oder 2,5 % (Art. 64), Konformität als Marktzugang

VO (EU) 2024/2847: Art. 13, 14, 64, 71, Anhang I



Drei Schwachstellen

Funktionstrennung	Überberechtigung	Zurechenbarkeit
Eine Person ändert Bankdaten und gibt die Zahlung frei.	SAP_ALL oder Notfallrechte dauerhaft vergeben, auch an persönliche Konten.	Sammelkonten und Dienstleisterzugänge ohne Zuordnung und ohne Entzug.



Wo die Leitung selbst gefordert ist

Gesellschaftsrecht

GmbH und AG

PFLICHT DER LEITUNG

Angemessenes IKS einrichten und überwachen

PERSÖNLICHE FOLGE

Schadenersatz gegenüber der Gesellschaft (§ 25 GmbHG, § 84 AktG)

NISG 2026

erfasste Einrichtungen

PFLICHT DER LEITUNG

Einhaltung sicherstellen und beaufsichtigen, Schulungspflicht (§ 31 NISG)

PERSÖNLICHE FOLGE

Wesentliche Einrichtungen: Untersagung der Leitung möglich (§ 39 NISG)

DORA

Finanzunternehmen

PFLICHT DER LEITUNG

Letztverantwortung für das IKT-Risikomanagement (Art. 5)

PERSÖNLICHE FOLGE

Aufsichtsrechtliche Folgen nach nationalem Recht



Wann haften Geschäftsführung und Vorstand?

Pflichtverletzung → **Verschulden** → **Kausalität** → **Schaden der Gesellschaft**

Keine Erfolgshaftung

Fehlverhalten von Mitarbeitenden macht die Leitung nicht automatisch haftbar. Im OGH-Fall wurde der Geschäftsführer entlastet.

Aber: Organisation zählt

Schuldhaft unterlassene Organisation oder Überwachung kann genügen. Zugriffsbeschränkungen nennt der OGH als Teil des IKS.

Innenhaftung gegenüber der Gesellschaft · OGH 8 ObA 109/20t · § 25 GmbHG · § 84 AktG



Im Haftungsprozess gegen Geschäftsführung oder Vorstand:

Ihre Sorgfalt müssen Sie beweisen.

Die Gesellschaft muss den Schaden und dessen adäquat kausale Verursachung darlegen.
Dass Sie sorgfältig gehandelt haben, müssen Sie nachweisen.

Im OGH-Fall gelang das: Der Geschäftsführer haftete nicht.

OGH 8 ObA 109/20t, Rz 51, 80 · § 84 Abs. 2 AktG



Risiko akzeptieren: ja. Rechtsverstoß: nein.

Ihr Spielraum

Business Judgment Rule

Angemessen informiert, frei von sachfremden Interessen, vertretbar zum Wohl der Gesellschaft

Wahl zwischen rechtlich geeigneten Lösungen

Ausnahmen mit Ersatzkontrolle, Begründung und jährlicher Wirksamkeitsprüfung (§ 4 NISV)

Kein Spielraum

Zwingendes Recht

Pflichten wie Art. 32 DSGVO oder § 32 NISG

Kosten zählen bei der Angemessenheit, rechtfertigen aber keinen feststehenden Verstoß

Eine D&O- oder Cyberversicherung ersetzt keine Organpflicht

§ 25 Abs. 1a GmbHG · § 84 Abs. 1a AktG · OGH 6 Ob 35/19v · § 4 NISV 2026



Zurück zum Fall: mögliche Entlastungsnachweise

	IM FALL	MÖGLICHER ENTLASTUNGSNACHWEIS
U	Vertretungsrechte nie entzogen	**Entzug nach Ende der Vertretung, regelmäßige Rechteprüfung**
U	Bankdatenänderung ohne Prüfung	**Vier-Augen-Freigabe oder Rückruf beim Lieferanten**
L	Management Letter ohne Beschluss	**Bewertung, Verantwortliche, Frist: dokumentierte Entscheidung**
L	Behebung auf „S/4“ verschoben	**Befristete Ausnahme mit Ersatzkontrolle und Wirksamkeitsbericht**

U = Ebene Unternehmen **L** = Ebene Leitung · Die entlastenden Unterlagen entstehen jetzt, nicht erst danach.

Fiktiver Praxisfall



BI§ET

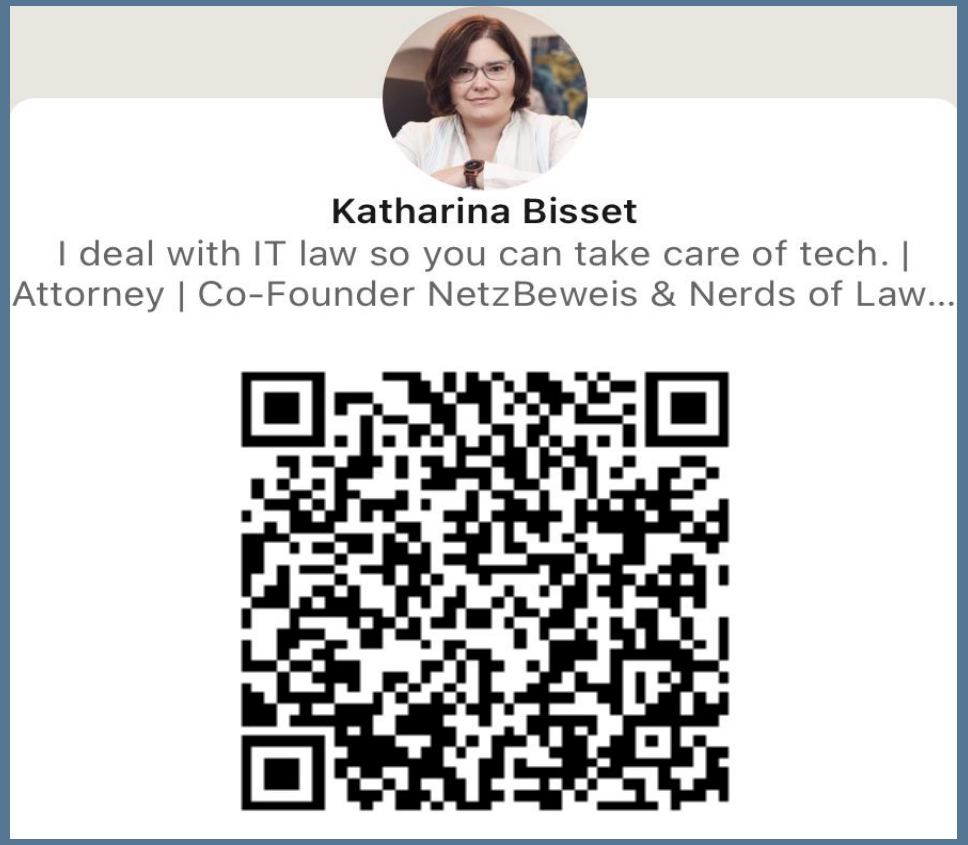
Vier Fragen für Ihre Geschäftsleitung

1. Welche Regelwerke gelten, und ist eine allfällig nötige NISG-Registrierung erledigt?
2. Welche kritischen Rechte und offenen Prüfhinweise haben wir?
3. Wer behebt sie bis wann, und wer prüft, ob es wirkt?
4. Könnten wir unsere heutige Entscheidung später belegen?

Morgen: einen kritischen Prozess wählen und den letzten Prüfhinweis bis zum Abschluss verfolgen.



Danke für Ihre Aufmerksamkeit!



Hauptstraße 38
2452 Mannersdorf am Leithagebirge

office@bisset.at www.bisset.at

+43 660 470 8771