NAVIGIEREN IM CYBERRECHT:

ISG, NIS2 UND COMPLIANCE FÜR DIE SCHWEIZ

Webinar, 24. Oktober 2024

Simon T. Oeschger
lic. iur., Rechtsanwalt, MAS MTEC ETHZ
simon.oeschger@snplegal.com

SN&P Suffert Neuenschwander & Partner

1. KONTEXT UND EINORDNUNG

Informations- und Cybersicherheit in der Schweiz und in Europa (Auswahl)

Datenschutzgesetz (DSG)

- In Kraft seit: 1. Sept 2023
- Schutz von Personendaten in der Schweiz

Informationssicherheits-gesetz (ISG)

- In Kraft seit: 1. Jan 2024
- Revision ISG: 1. Jan 2025 (geplant)
- Cybersicherheit und Umsetzung nationale Cyberstrategie

FINMA Empfehlungen in Aufsichtsmitteilungen

- 03/2024 «Cyber-Risiken»
- 04/2024«Management der operat. Risiken»
- 02/2020 «Meldepflicht Cyber-Attacken gem. Art.29 Abs. 2 FINMAG»

FINMA Anforderungen in Rundschreiben

- RS 2018/3 «Auslagerungen – Banken […] nach FINIG»
- RS 2023/1: «Operat. Risiken und Resilienz – Banken»

Branchenspezifische Regulierungen

- BG über die Fernmelde-unternehmen (FMG)
- BG über die Überwachung von Post- und Fernmeldewesen (BÜPF)
- Etc.

Datenschutzgrundver-ordnung (DSGVO)

- In Kraft seit: 25. Mai 2018
- Schutz von Personendaten in Europa

NIS 2-Richtlinie

- In Kraft seit: 27. Dez 2022
- Umsetzungsfrist in nationales Recht: 17. Oktober 2024
- Massnahmen für ein hohes gemeinsames Cybersicherheits-niveau in der EU

Digital Operational Resilience Act (DORA)

- In Kraft seit: 16. Januar 2023
- Umsetzungsfrist bis: 16. Januar 2025
- Digitale operationelle Resilienz im Finanzsektor

Cyber Security Act (CSA)

- In Kraft seit: 27. Juni 2019
- Massnahmen zur Stärkung der EU gegen Cyberangriffe
- EU-weites Zertifizierungssystem

Cyber Resilience Act (CRA)

- In Kraft: Ende 2024 (geplant)
- Übergangsfrist: 21 / 36 Monate
- Cybersicherheit in Hardware und Software-Produkte sowie IoT-Produkten

SN&P Suffert Neuenschwander & Partner

1. KONTEXT UND EINORDNUNG

Schutzobjekt

- **Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)**

  Art. 1 – Zweck

  Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.

- **Bundesgesetz über die Informationssicherheit (Informationssicherheitsgesetz, revISG)**

  Art. 1 – Zweck

  Abs. 1: Dieses Gesetz soll:

  a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten;

  b. die Widerstandsfähigkeit der Schweiz gegenüber Cyberbedrohungen erhöhen.

  Abs. 2: Dadurch sollen die folgenden öffentlichen Interessen geschützt werden:

  a. die Entscheidungs- und Handlungsfähigkeit der Behörden und Organisationen des Bundes;

  b. die innere und äussere Sicherheit der Schweiz;

  c. die aussenpolitischen Interessen der Schweiz;

  d. die wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz;

  e. die Erfüllung der gesetzlichen und vertraglichen Verpflichtungen der Behörden und Organisationen des Bundes zum Schutz von Informationen

1. KONTEXT UND EINORDNUNG

Informationssicherheit vs. Datenschutz: Unterschied

Informationssicherheit

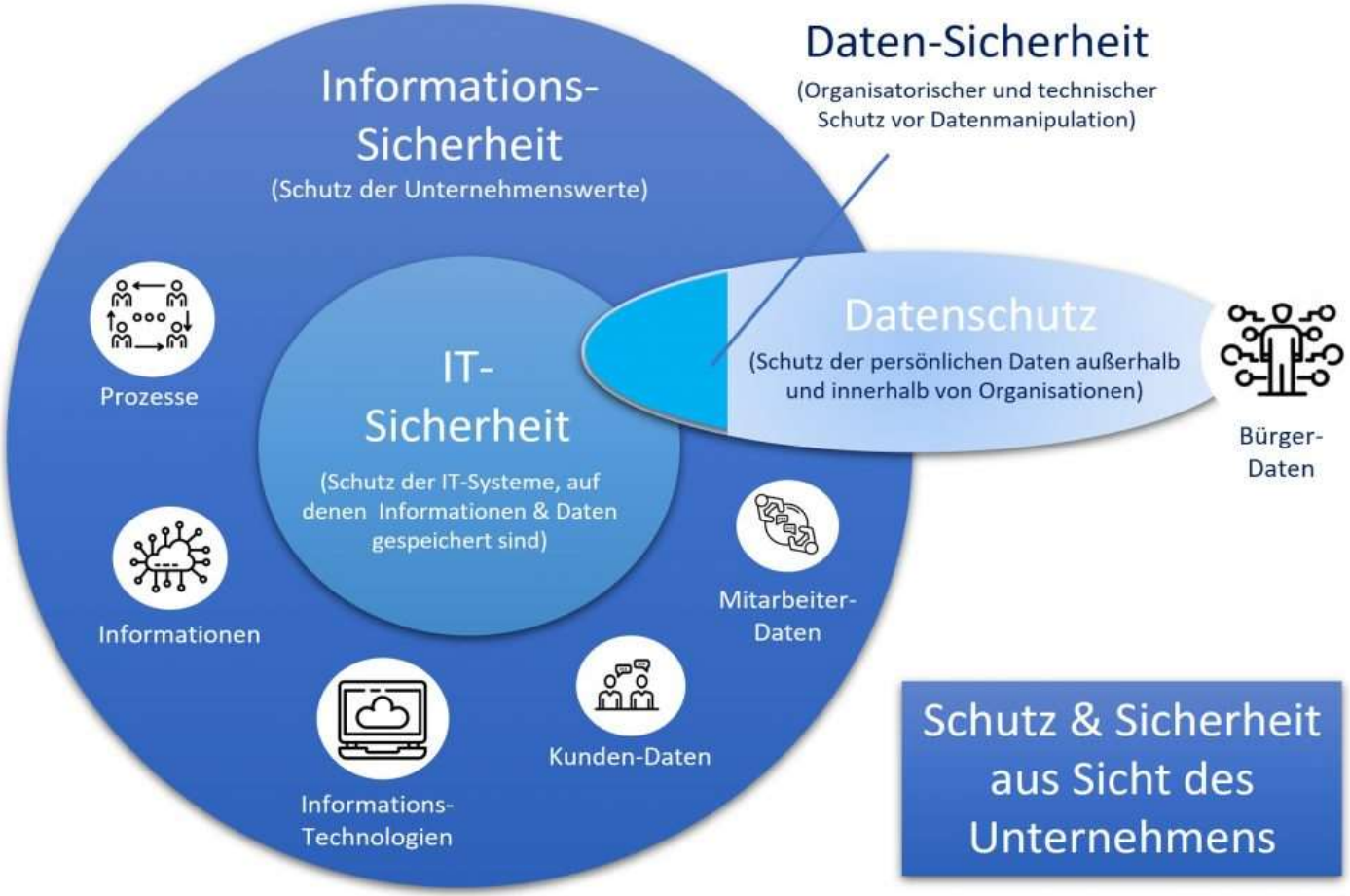
- **Schutz von Daten** und **datenverarbeitenden, technischen Systemen**
- Die **Schutzziele** sind, die **Vertraulichkeit, Verfügbarkeit und Integrität der Daten** zu erhalten sowie die **Authentizität, Nachvollziehbarkeit und die Verbindlichkeit** bei der Bearbeitung von Daten zu erhalten.
- Umsetzung von **technischen und organisatorischen Massnahmen** zum Schutz der Systeme und Daten

Kontext zum Datenschutz:
Schutzniveau für Daten führt zur Erhöhung des Personen-Datenschutzes bei Behörden

Datenschutz

- Schutz des **Grundrechts auf informationelle Selbstbestimmung** von Einzelpersonen (**Art. 13 Abs. 2 BV**; Persönlichkeitsschutz), wonach jeder selbst bestimmen können soll, wem er wann welche seiner Daten zu welchem Zweck zugänglich macht.
- Es geht somit um den **Schutz der Person bzw. der Persönlichkeit**.
- Datenschutzgesetz (DSG) regelt für private Personen sowie für Bundesorgane, **ob Personendaten erhoben, verarbeitet oder gespeichert werden dürfen oder nicht**.
(DSG als lex specialis zum ISG)

1. KONTEXT UND EINORDNUNG



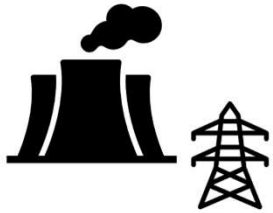
Bildquelle: www.vialevo.de

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Wen betrifft das ISG?

verpflichtete Behörden und Organisationen (Definition Art. 2 f. ISG)

Dritte Parteien, wie Dienstleister und Partner
z.B. Unternehmen, die Zugang zu sensiblen Informationen haben oder kritische Systeme unterstützen



Betreiber kritischer Infrastrukturen und grundlegender Dienstleistungen
z.B. Energie, Wasser, Verkehr, Gesundheit, Telekom, etc.

ISG

Private Unternehmen, die Verwaltungs-aufgaben übernehmen, in sensiblen Bereichen tätig sind oder mit kritischen Infrastrukturen verbunden sind
z.B. Unternehmen der Finanzbranche, Dienstleister von kritischen Infrastrukturen

Behörden Bund/Kantone/Gemeinden und weitere Organisationen
z.B. Departemente, Gerichte, Armee, etc.

SN&P Suffert Neuenschwander & Partner

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Wen betrifft das ISG?

Wichtig: Dienstleister können indirekt dem ISG unterliegen!

Art. 9 – Zusammenarbeit mit Dritten

Abs. 1: Arbeiten die verpflichteten Behörden und Organisationen mit Dritten zusammen, so sorgen sie dafür, dass die Anforderungen und Massnahmen nach diesem Gesetz in den entsprechenden Vereinbarungen und Verträgen festgehalten werden.

Abs. 2: Sie sorgen für eine angemessene Überprüfung der Umsetzung der Massnahmen.

Die **Folge für Zulieferer oder Dienstleistungsunternehmen** von verpflichteten Behörden oder Organisationen ist,

- dass sie eine Pflicht zum Ergreifen von Sicherheitsmassnahmen zum Schutz ihrer Dienste und der Daten treffen müssen.

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Neuregelung im revISG: Meldung von Cyber-Angriffen

- Freiwillige Meldung bei Cyber-Vorfällen (inkl. Cyber-Bedrohungen) und Schwachstellen in Informatikmitteln (Art. 73b revISG):
  - **Meldestelle: Bundesamt für Cybersicherheit (BACS)** [bisher: National Cyber Security Centre NCSC]
  - Melderecht nicht auf Betreiber kritischer Infrastrukturen beschränkt, sondern steht jeder Person offen (kann auch anonym erfolgen)

- Meldepflicht bei Cyber-Angriffen (Art. 74a-e revISG):
  - Pflicht zur Meldung an BACS für **Betreiber kritischer Infrastrukturen** bzw. meldepflichtige Behörden und Organisationen **innerhalb von 24 Stunden** seit deren Entdeckung von Cyber-Angriffen, **sofern sie schwerwiegende Auswirkungen** haben.

- Verletzung der Meldepflicht (Art. 74g-74h revISG):
  - Bei vorsätzlicher Pflichtverletzung durch meldepflichtige Behörde oder Organisation, kann der Verantwortliche mit einer **Busse von bis zu CHF 100 000.–** bestraft werden.

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Meldepflicht bei Cyber-Risiken (revISG) für wen? (1/3)

- Meldepflicht bei Cyber-Angriffen (Art. 74a-e revISG) erheblich weiter gefasst als Behörden und Organisationen i.S.v. Art. 2 ISG und verpflichtet:
  - **Hochschulen**;
  - **Bundes-, Kantons- und Gemeindebehörden** sowie interkantonale, kantonale und interkommunale Organisationen;
  - Organisationen mit öffentlichen Aufgaben in den Bereichen **Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung** (soweit sie hoheitlich handeln);
  - **Energieversorger** und in den Energieversorgung Energiehandel, Energiemessung oder Energiesteuerung tätige Unternehmen;
  - **Banken, Privatversicherungen und Finanzmarktinfrastrukturen**
  - **Gesundheitseinrichtungen auf der kantonalen** Spitalliste (neben Spitälern auch Geburtshäuser und Pflegeheime);
  - **medizinische Laboratorien** mit einer Bewilligung nach dem Epidemiengesetz;
  - **Unternehmen, die Arzneimittel herstellen, Inverkehrbringen oder Einführen;**
  - **Sozialversicherer**
  - **die SRG und Nachrichtenagenturen von nationaler Bedeutung** (derzeit nur noch Keystone-SDA);

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Meldepflicht bei Cyber-Risiken (revISG) für wen? (2/3)

- **Postdienstanbieter**;
- **Eisenbahnunternehmen und Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen;**
- Unternehmen der **Zivilluftfahrt** und **Landesflughäfen** gemäss Sachplan Infrastruktur;
- Bestimmte Schifffahrtsunternehmen (Rhein und Hafen Basel);
- Unternehmen, welche die Bevölkerung mit **unentbehrlichen Gütern des täglichen Bedarfs versorgen** und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen führen würde
- registrierte **Fernmeldedienstanbieterinnen**;
- **Registrare**;
- Anbieter und Betreiber von Diensten und Infrastrukturen, die der **Ausübung der politischen Rechte** dienen (E-Voting, Systeme zur Führung von Stimmregistern etc.);
- **Anbieter und Betreiber von Cloudcomputing, Suchmaschinen, digitalen Sicherheits- und Vertrauensdiensten sowie Rechenzentren** mit Sitz in der Schweiz
- **Hersteller von Hard- oder Software**, deren Produkte von kritischen Infrastrukturen genutzt werden und einen Fernwartungszugang haben oder eingesetzt werden zur Steuerung und Überwachung von betriebstechnischen Systemen und Prozessen oder zur Gewährleistung der öffentlichen Sicherheit.

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Meldepflicht bei Cyber-Risiken (revISG) für wen? (3/3)

- **Ausnahmen von der Meldepflicht** bei Cyber-Angriffen nach Art. 74b revISG geregelt in **Art. 16 CSV-Entwurf**:
  - **Nicht meldepflichtig sind vereinfacht ausgedrückt alle Behörden und Unternehmen, bei denen ein Cyberangriff keine unmittelbaren Auswirkungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung hat.**
  - Unternehmen mit weniger als 50 Mitarbeitenden, einem Jahresumsatz oder einer Jahresbilanzsumme von weniger als 10 Millionen Franken (Art. 16 Abs. 2 CSV-Entwurf).
  - Behörden, die für weniger als 1000 Einwohnerinnen und Einwohner zuständig sind (Art. 16 Abs. 1 lit. a CSV-Entwurf).
  - Unternehmen aus dem Bereich kritische Infrastrukturen, die branchenspezifische Schwellenwerte unterschreiten (Art. 16 Abs. 1 lit. b, c und d CSV-Entwurf). Zum Beispiel Eisenbahnbetriebe ohne Personenbeförderungskonzession oder Netzbetreiber, die weder das Schutzniveau A oder B haben.
  - **Meldepflichtig sind damit ab Inkrafttreten beispielsweise Bundes-, Kantons- und grössere Gemeindebehörden, Organisationen in den Bereichen Sicherheit und Rettung, Trinkwasser- und Energieversorgung, aber auch Banken, Hochschulen oder die SBB.**

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Welche Anforderungen und Pflichten regelt das ISG?

- Anforderungen an verpflichtete Organisationen und Behörden (Definition Art. 2 ISG) betreffend Informationssicherheit, u.a. (Art. 6-26 ISG):
  - **Informationssicherheits-Management-System (ISMS) erstellen und umsetzen**, welches die Anforderungen des ISG erfüllt; u.a. Beurteilung Schutzbedarf der Informationen (Art. 6), ggf. deren Klassifizierung (Art. 11-15) etc.
  - **Etablierung Risikomanagement (Art. 8):**
    Identifikation und Beurteilung von Risiken, Umgang mit identifizierten Risiken festlegen, Massnahmen treffen (TOM, z.B. Zugriffskontrolle, Datenverschlüsselung, Firewall-/Netzwerksicherheit, Antivirus- und Malware-Schutz), sowie die Wirksamkeit der Massnahmen regelmässig prüfen
  - **Informatikmittel (Art. 16-19)**: Festlegen von Sicherheitsverfahren bei Informatikmitteln, inkl. Zuordnung des Schutzniveaus

2. INFORMATIONSSICHERHEITSGESETZ (ISG)

Welche Anforderungen und Pflichten regelt das ISG?

- Anforderungen an verpflichtete Organisationen und Behörden (Definition Art. 2 ISG) betreffend Informationssicherheit, u.a. (Art. 6-26 ISG):
  - **Personal (Art. 20)**: sorgfältige Auswahl, Identifikation und Sicherheitsüberprüfung, Weiterbildung und Schulung
  - **Physischer Schutz betr. Räumlichkeiten und Bereiche (Art. 22-23)**: Risiken reduzieren, die von physischen Bedrohungen (menschliche Handlungen, Elementarschäden) ausgehen. Räumlichkeiten und Bereiche Sicherheitszonen zuordnen und Kontrollen einsetzen
  - **Zusammenarbeit mit Dritten (Art. 9)**: Bei Dritten, die nicht dem ISG unterstehen, ist dafür zu sorgen, dass bei der Auftragserteilung und -ausführung die gesetzlichen Massnahmen Sicherheitsmassnahmen vertraglich geregelt und eingehalten werden.

3. NETWORK AND INFORMATION SECURITY (NIS 1, NIS 2)

Wen betrifft die NIS 2-Richtlinie?

- **Die Sektoren von NIS 1 auf die folgenden 16 Sektoren ausgeweitet:**
  - **Weiterhin**: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, digitale Infrastruktur
  - **Neu**: Abwasser, ICT-Service Management B2B, öffentliche Verwaltung, Weltraum, wichtige Einrichtungen wie Post- und Kurierdienste, Abfallbewirtschaftung, Chemie, Lebensmittel, verarbeitendes/herstellendes Gewerbe
  - **Neu, fakultativ**: Anbieter digitaler Dienste und Research Organisationen
- **Ausgenommen:**
  - Unternehmen < 50 Mitarbeitenden, Jahresumsatz < 10 Mio EUR oder Jahresbilanzsumme < 10 Mio EUR;
  - **Gegenausnahme:** alleiniger Anbieter kritischer Aktivitäten im Mitgliedstaat

3. NETWORK AND INFORMATION SECURITY (NIS 1, NIS 2)

Meldepflichten und Sanktionen bei Verstoss

- **Meldepflicht bei signifikanten Sicherheitsvorfällen**
  - Meldepflicht **binnen 24 Stunden Frühwarnung** und **innerhalb von 72 Stunden eine Einschätzung** an die Behörde

- **Sanktionen**
  - **Bussen bis zu 10 Mio. EUR und 2 Prozent des Gesamtjahresumsatzes des Konzerns bei wesentlichen Einrichtungen** bzw. 7 Mio EUR und 1,4 Prozent des Gesamtjahresumsatzes des Konzerns bei wichtigen Einrichtungen.
  - **Führungskräfte** (CEOs bzw. Verwaltungsräte) können in Zukunft für die Nichtumsetzung **zur Verantwortung gezogen** werden.

3. NETWORK AND INFORMATION SECURITY (NIS 1, NIS 2)

Zusammenfassung und Empfehlungen

- Die EU-Richtlinie NIS 2 muss von den EU/EWR Ländern bis 17. Oktober 2024 in nationale Gesetzgebung umgesetzt werden
  - 18 Sektoren (Branchen) sind NIS 2 relevant.
  - Die Beurteilung auf NIS 2 Betroffenheit erfolgt auf Basis der Schwellenwerte im jeweiligen Land.
  - Für Deutschland wird die NIS 2 Umsetzung in den nächsten Monaten erwartet.

- **Empfehlung:** Schweizer Unternehmen müssen ihre NIS 2-Betroffenheit abklären:
  - **Sektor:** Prüfung, ob Tätigkeiten in EU/EWR unter NIS 2 fallen
  - **EU Länder / Schwellenwerte:** Prüfung der Schwellenwerte in relevanten Ländern
  - **Lieferkettengesetze:** Prüfung, ob Kunden unter NIS 2 fallen und von ihren Lieferanten Nachweise für Cybersicherheit verlangen.
  - **Falls keine NIS 2-Betroffenheit:** Prüfung, ob Cybersicherheit im Unternehmen auf Stand der Technik ist

ADD-ON

Weiterführende Links unter Berücksichtigung der Teilnehmerfragen im Webinar

- BACS Meldestelle für Cyber-Vorfälle: https://www.report.ncsc.admin.ch/de/

- BACS Dokumentationen und Hilfestellungen:
  - **Informatiksicherheitsvorgaben Bund**:
    - https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund.html
  - **Vorgaben des BACS** zur Schutzbedarfsanalyse, zum IKT-Grundschutz, etc.:
    - https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/beurteilung-schutzbedarf.html
    - https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html

SN&P Suffert Neuenschwander & Partner

Simon T. Oeschger

lic. iur. Rechtsanwalt
MAS MTEC ETHZ, CAS Cyber Sicherheit UZH

Spezialisierter Rechtsanwalt in Wirtschafts-, IT/Technologierecht und Datenschutz

simon.oeschger@snplegal.com
www.snplegal.com

DISCLAIMER

Die Folien dieser Präsentation beinhalten generische Informationen und beziehen sich auf keinen konkreten Sachverhalt oder auf konkrete Umstände eines Falles.

Diese Präsentation gibt ausschliesslich die persönliche Meinung des/der Autoren wieder. Die Inhalte sollen nicht als spezifischer Rat oder rechtliche Abklärung verstanden werden. Wenn Sie eine rechtliche Beratung zu diesem oder einem anderen Thema benötigen, wenden Sie sich bitte an Ihren Anwalt bei SNPlegal, der Ihnen helfen kann, eine auf Ihre spezielle Situation zugeschnittene rechtliche Beratung zu erhalten.

Es gilt das gesprochene Wort.