DATENSCHUTZ & NETZ- UND INFORMATIONSSICHERHEIT
in der EU

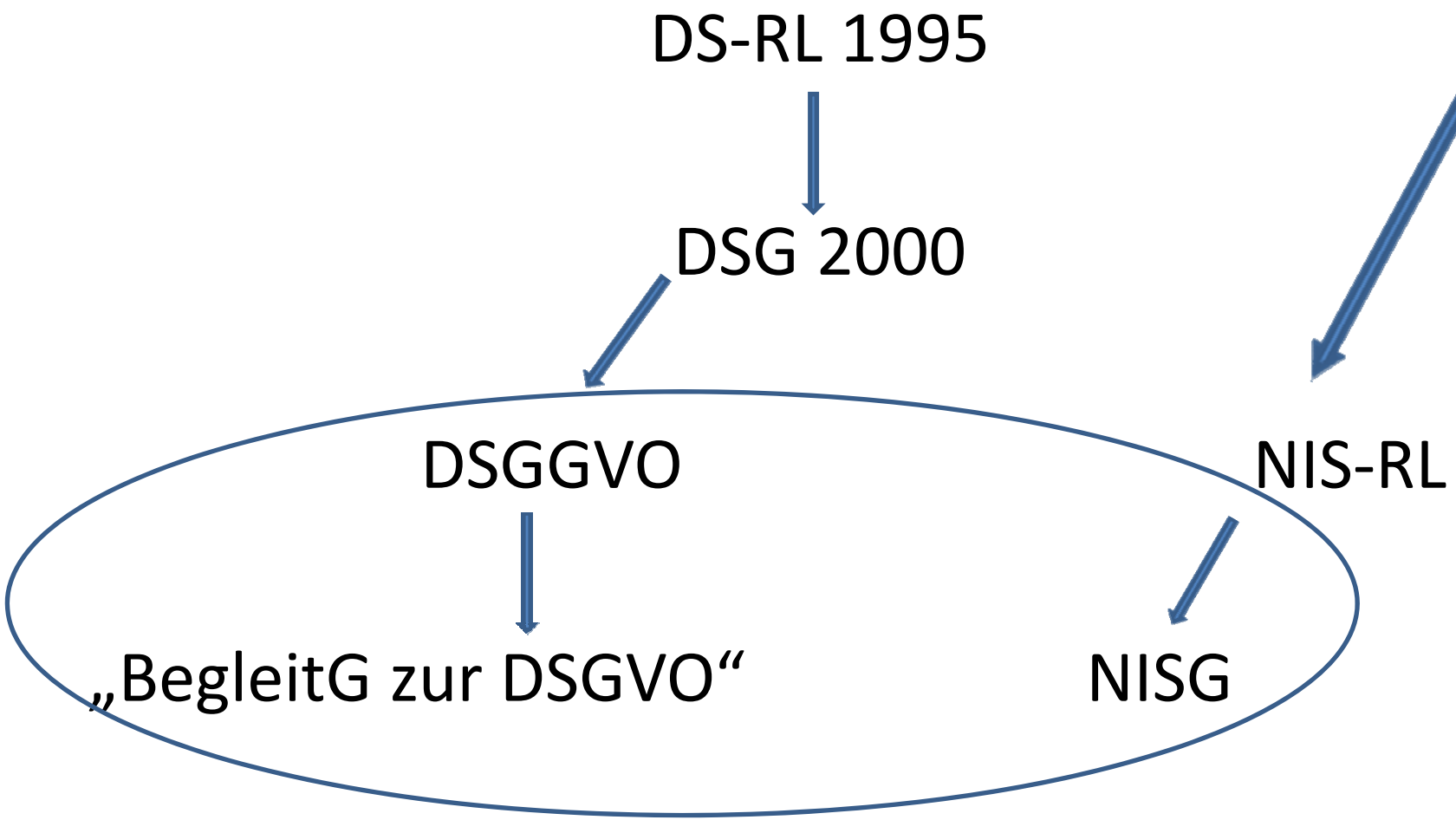
Peter Burgstaller
Rechtsanwalt, Linz
Professor for IT- and IP-Law
University of Applied Science Upper Austria

Verschränkung von Daten- und Informationssicherheit

- Datenschutz – personenbezogene Daten
- Informationsschutz umfasst alle Daten, insb auch Betriebs-/Geschäftsgeheimnis
- Datenschutz ist eine Teilmenge des Informationsschutzes
- DSGVO + NIS-RL sehen insb die Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit vor

Confidentiality **I**ntegrity **A**vailability

NEUES DATEN- UND INFORMATIONSSICHERHEITSRECHT ab 5/2018



A. Datenschutz-Grundverordnung (DSGVO 2016)

ECKDATEN:

- April 2016 beschlossen das EP und der Rat die DSGVO
- Per 25.05.2018 tritt eine **vereinheitlichte** und neue Datenschutzregelung in Kraft und ersetzt die DS-RL 1995
- Datenschutzmaßnahmen müssen in die Produkte integriert werden= **Datenschutz durch Technikgestaltung**
- **Datenschutz durch datenschutzfreundliche Voreinstellungen** = vor der Verarbeitung von personenbezogenen Daten muss die betroffene Person dies genehmigen (z.B.: Einführung von Cookies)
- **Sicherheit personenbezogener Daten** = der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen (TOMs), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem ein:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - Sicherstellung von **Vertraulichkeit/Integrität/Verfügbarkeit und Belastbarkeit** = **I**nformations**S**icherheits**M**anagement**S**ystem

DSGVO 2016

ECKDATEN:

- Keine Meldung beim DVR
- Internes Datenverarbeitungsverzeichnis
  - > 250 Arbeitnehmer bzw
  - Informationspflicht an Betroffenen
- Akteure:
  - Betroffener
  - Verantwortlicher
  - Auftragsdatenverarbeiter
- Datenschutzbeauftragter in bestimmten Bereichen

Sachlicher Anwendungsbereich

- DSGVO findet Anwendung auf:
  - die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten
  - die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (nicht manuell und unstrukturierte Datenverarbeitung)

- DSGVO findet keine Anwendung auf die Verarbeitung personenbezogener Daten:
  - Insb durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des **Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit**.

Verarbeitungsgrundsätze

Personenbezogene Daten müssen

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (**„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“**);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; (**„Zweckbindung“**);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (**„Datenminimierung“**);
- sachlich richtig sein (**„Richtigkeit“**);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es erforderlich ist (**„Speicherbegrenzung“**);
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (**„Integrität und Vertraulichkeit“**).

Der Verantwortliche ist für die Einhaltung dieser Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können (**„Rechenschaftspflicht“**).

Rechtmäßige Verarbeitung

Die Verarbeitung ist nur rechtmäßig, wenn

- die betroffene Person ihre Einwilligung zu der Verarbeitung gegeben hat
- die Verarbeitung zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist,
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt;
- die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt;
- die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Bedingungen für Einwilligung

- Der Verantwortliche muss nachweisen, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung auf eine Weise erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.
- Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.
- Kinder unter 16 Jahren (die Mitgliedsstaaten können die Altersgrenze auf 13 Jahre herabsetzen) können nur mit Zustimmung der Eltern einwilligen.

Verarbeitung besonderer Kategorien(a)

- Die Verarbeitung von Daten die die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.
- Ausnahmen:
  - Die betroffene Person hat **ausdrücklich** für einen oder mehrere festgelegte Zwecke eingewilligt
  - Die Verarbeitung ist **im Bereich des Arbeitsrechts** und dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich

Verarbeitung besonderer Kategorien(b)

- Ausnahmen:
  - die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich
  - die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten
  - die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,
  - die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,
  - die Verarbeitung ist aus **Gründen eines erheblichen öffentlichen Interesses erforderlich**,
  - die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich,
  - die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich

Rechte der betroffenen Person

- Informationsrecht
- Auskunftsrecht
- Berichtigungsrecht – Recht auf Vergessen
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

Pflichten des für die Verarbeitung Verantwortlichen

- Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen (TOMs) umsetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt
- Der Verantwortliche kann die Einhaltung eines genehmigtes Zertifizierungsverfahren als Gesichtspunkt heranziehen, um die Erfüllung seiner Pflichten nachzuweisen
- Der Verantwortliche muss geeignete TOMs treffen, wie z. B. Pseudonymisierung, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen **= Datenschutz durch Technikgestaltung**
- Der Verantwortliche muss geeignete TOMs treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden **= Datenschutz durch datenschutzfreundliche Voreinstellungen**
- Der Verantwortliche muss mit Auftragsverarbeitern arbeiten, die hinreichend Garantie dafür bieten, dass geeignete TOMs umgesetzt werden
- Jeder Verantwortliche führt ein schriftliches (inkl. elektronisches Format) Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen (Informationsrecht der betroffenen Person).

Pflichten des Auftragsverarbeiters

- Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der **Grundlage eines Vertrags** nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten, der den Verantwortlichen bindet und festlegt:
  - Gegenstand und Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - Art der personenbezogenen Daten und Kategorien der betroffenen Personen und
  - Pflichten und Recht des Verantwortlichen
- Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags auferlegt, die in dem Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind.
- Der **Vertrag ist schriftlich abzufassen**, was auch in einem elektronischen Format erfolgen kann.
- Der Auftragsverarbeiter nimmt **keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch**.
- Jeder Verantwortliche und Auftragsverarbeiter führt ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen (Informationsrecht des Betroffenen). Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

Verarbeitungsverzeichnis

- Verantwortlicher und Auftragsverarbeiter haben eine Verarbeitungsverzeichnis zu führen (ersetzt DVR-Meldung)
- Nur wenn mehr als 250 Beschäftigte
- Inhalt nach Art 30 DSGVO:
  - Art der Daten
  - Zweck
  - Art der Verarbeitung uvm

Sicherheitsmaßnahmen

Technische Organisatorische Maßnahmen

- Der Verantwortliche und der Auftragsverarbeiter treffen geeignete TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese schließen unter anderem Folgendes ein:
  - die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs zur Gewährleistung der Sicherheit der Verarbeitung.
- TOMs zur Vermeidung von Sicherheitsverletzungen, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden
- Der Verantwortliche kann die Einhaltung eines genehmigtes Zertifizierungsverfahren als Gesichtspunkt heranziehen, um die Erfüllung seiner Pflichten nachzuweisen

Meldung von Verletzungen des Schutzes personenbezogener Daten

- Der Verantwortliche meldet im Falle einer Verletzung des Schutzes personenbezogener Daten möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde, diese **der zuständigen Aufsichtsbehörde**, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Die Meldung enthält zumindest eine Beschreibung der Art der Verletzung, mit Angabe der Kategorien und der Zahl der betroffenen Personen und der personenbezogenen Datensätze, Kontaktdaten des Datenschutzbeauftragten, wahrscheinliche Folgen, bereits ergriffene Maßnahmen
- Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Datenschutz-Folgenabschätzung und vorherige Konsultation (a)

- Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch, insbesondere in folgenden Fällen
  - systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
  - umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten oder
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
- Der Verantwortliche holt sich den Rat des Datenschutzbeauftragten ein. (DSB)

Datenschutz-Folgenabschätzung und vorherige Konsultation (b)

- Wenn die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung stünde, unterbreitet sie dem Verantwortlichen **innerhalb eines Zeitraums von bis zu acht Wochen** nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen (z.B.: Verbot der Verarbeitung)
- Falls die Aufsichtsbehörde nicht der Auffassung ist, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung stünde, unterbreitet sie keine solche schriftlichen Empfehlungen

Datenschutzbeauftragter(DSB)

- Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten und übermitteln der Behörde Kontaktdaten, wenn:
  - die Verarbeitung von einer **Behörde oder öffentlichen Stelle** durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
  - die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen** erforderlich machen, oder
  - die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung **besonderer Kategorien von Daten** oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.
- Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen

Übermittlungen an Drittländer

- Keine besondere Genehmigung hinsichtlich Ländern mit angemessenem Schutzniveau => Beschluss der Kommission und laufende Überwachung (z.B. Neuseeland, Norwegen, Schweiz, Island, Argentinien, Uruguay, Guernsey Inseln, Jersey, Isle of Man) oder
- Falls kein solcher Beschluss vorliegt, dürfen personenbezogene Daten nur übermittelt werden, wenn geeignete Garantien vorgesehen sind, der betroffenen Person durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen und sich der Datenimporteur dazu verpflichtet (Safe Harbour mit Kanada und Israel bzw EU-US-Privacy Shield) oder
- Garantien und Genehmigung der zuständigen Behörde

C. GTelG 2012

GTelG - § 3:

Gesundheitsdiensteanbieter dürfen Gesundheitsdaten nur dann (elektronisch) weitergeben, wenn

1. die Weitergabe zu einem in § 9 DSG 2000 angeführten Zweck zulässig ist und
2. die Identität (§ 4) jener Personen, deren Gesundheitsdaten weitergegeben werden sollen, nachgewiesen ist und
3. die Identität (§ 4) der an der Weitergabe beteiligten Gesundheitsdiensteanbieter nachgewiesen ist und
4. die **Rollen** (§ 5) der an der Weitergabe beteiligten Gesundheitsdiensteanbieter nachgewiesen sind und
5. die **Vertraulichkeit** (§ 6) der weitergegebenen Gesundheitsdaten gewährleistet ist sowie
6. die **Integrität** (§ 7) der weitergegebenen Gesundheitsdaten gewährleistet ist.

=> IT-Sicherheitskonzept = Doku über die Datensicherheitsmaßnahmen

D. NIS-RICHTLINIE

- Die Richtlinie (EU) 2016/1148 des europ. Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL), seit **08.08.2016 in Kraft**.
- Nach Art 25 NIS-RL werden die Mitgliedstaaten **bis zum 09.05.2018** die Rechts- und entsprechenden Vorschriften erlassen und veröffentlichen, um die Richtlinie umzusetzen => **NIS-Gesetz**
- Ab 10.05.2018 wenden die Mitgliedstaaten diese Maßnahmen an.

1. NIS-Richtlinie

Die Mitgliedsstaaten gewährleisten, dass

- Öffentliche Verwaltungen und
- Anbieter von
  - kritischen Infrastrukturen und
  - Dienste der Informationsgesellschaft

geeignete technische und organisatorische Maßnahmen (=TOM) ergreifen, um die Risiken für die Sicherheit der Netze und Informationssysteme zu managen

=>**InformationsSicherheits-ManagementSystem**

(vgl auch die Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen der DSGVO)

2. NIS-Richtlinie

a) Mitgliedstaaten gewährleisten, dass

- Öffentliche Verwaltungen und
- Anbieter von kritischen Infrastrukturen und digitalen Diensten

den nationalen NIS-Behörden **Sicherheitsvorfälle melden**, die **erhebliche Auswirkungen** auf die Sicherheit haben.

b) Die Mitgliedstaaten gewährleisten, dass die

NIS-Behörde die Öffentlichkeit über Sicherheitsvorfälle, die im öffentlichen Interesse liegen, unterrichtet

3. Betreiber kritischer Infrastrukturen (Anhang 2 NIS-RL)

1. Energie – Strom, Kernkraft, Öl, Gas, Verteilersysteme, Speichersysteme, Raffinations- und Behandlungsanlagen
2. Verkehr – Luftfahrtunternehmen, Eisenbahnen, Beförderungsunternehmen des Seeverkehrs, Häfen, Flughäfen, Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen
3. Bankwesen
4. Finanzmarktinfrastrukturen, Börsen
5. Gesundheitswesen

Krit. Infrastruktur-Liste

- MS müssen **bis 09.11.2018** ermittelt und nach 09.05.2018 alle 2 Jahre überprüft und ggf aktualisiert werden
- Kriterien für die Ermittlung:
  - Dienst ist wesentlich für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten
  - Dienst hängt von Netz- und Informationssystemen ab
  - Ein Sicherheitsvorfall hätte signifikante Auswirkungen auf die weitere Bereitstellung des Dienstes

4. Anbieter von digitalen Diensten(Anhang 3 NIS-RL)

1. Online Marktplätze (Verträge über Waren und Dienstleistungen, zB auch App-Stores)
2. Suchmaschinen
3. Cloud-Computing-Dienste

⇒Nicht bei natürlichen Personen bzw Kleinstunternehmen

⇒Anbieter außerhalb EU müssen einen Vertreter benennen

Gemeinsame NIS-Standards

- Die Kommission stellt eine Liste einschlägiger Normen für die Netz- und Informationssicherheit auf und veröffentlicht diese (Art 16)

  => gibt Rechtssicherheit

- **ENISA** – Europäische Agentur für Netz- und Informationssicherheit (Sitz in Heraklion/Kreta/Griechenland) soll in allen Bereichen der NIS beraten (z.B.: Liste von Sicherheitsstandards)

Danke für Ihre Aufmerksamkeit!

Peter Burgstaller

office@lawfirm.eu