Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

Informationssicherheit für Volksschulen

Building Competence. Crossing Borders.

4. Oktober 2021

Herzlich Willkommen

Liebe Kurs-Teilnehmer des VSA

Herzlich Willkommen zur heutigen Veranstaltung zur Informationssicherheit für Volksschulen!

Schön, dass Sie hier sind, wir freuen uns auf die heutige Veranstaltung mit Ihnen!

Ihr ZHAW-Team

RA Dr. Michael Widmer & RA Marcel Griesinger

Agenda

Ihre heutige Agenda	
Abschnitt I.	Begrüssung und Vorstellung
Abschnitt II.	Einführung in das Datenschutzrecht
Kaffeepause von 14.45 bis 15.15 Uhr (Restaurant Piu)	
Abschnitt III.	Überblick zur Informationssicherheit, Tag 1
Abschnitt IV.	Aufgabe(n) und Ausblick für Tag 2

I. Begrüssung und Vorstellung

Ihre Dozenten am heutigen Tag

Rechtsanwalt
Dr. Michael Widmer
michael.widmer@zhaw.ch

Rechtsanwalt
Marcel Griesinger
marcel.griesinger@zhaw.ch

I. Begrüssung

Welche Berührungspunkte haben Sie bisher mit dem Thema Datenschutz & Informationssicherheit gehabt?

Bitte nehmen Sie sich einen kurzen Moment Zeit und notieren Sie Ihren Berührungspunkt auf der Padlet-Wall (Link nachfolgend):

https://padlet.com/marcelgriesinger/Bookmarks

I. Begrüssung

Konzept der drei «W-Fragen» bei der Erarbeitung rechtlicher Materie

- **«um was geht es?»**
- **«wo wird es relevant?»**
- **«was ist nun zu tun?»**

I. Begrüssung – Ausgangslage (“Ist-Zustand”)

- Die Digitalisierung führt im Lehr- und Bildungsbereich zu einem immer stärkeren Einsatz von IT-Anwendungen.
- Infolgedessen nehmen auch die damit verbundenen IT-spezifischen Risiken zu.
- Um diesen Risiken zu begegnen ist ein bewusster und strukturierter Umgang mit den Themen Informationssicherheit und Datenschutz notwendig.
- Durch klare Weisungen, ein hinreichendes Risikomanagement und gute Schutzmassnahmen lassen sich die anfallenden Risiken einschränken.

I. Begrüssung – Ausgangslage (Leitfaden)

- Um die Anwender bei der Begegnung der Risiken zu unterstützen wird der Leitfaden zur Informationssicherheit in Volksschulen herausgegeben.
- Anhand des Leitfadens besprechen wir mit Ihnen die Einführung, Umsetzung und Pflege einer nachhaltigen Informationssicherheit.
- Sie erhalten einen Überblick zu den gesetzlich geforderten Massnahmen zur Informationssicherheit.
- Zudem werden die von der kantonalen Datenschutzbeauftragten zur Verfügung gestellten Anleitungen und Vorlagen erläutert.

II. Einführung in das Datenschutzrecht

II. Einführung in das Datenschutzrecht

1. Überblick («um was geht es?)
2. Datenschutz und Schulbetrieb («wo wird es relevant?)
3. Erforderliche Umsetzungsmassnahmen («was ist zu tun?»)

II. Einführung in das Datenschutzrecht - Überblick

II. Einführung in das Datenschutzrecht - Überblick

170.4

Gesetz
über die Information und den Datenschutz (IDG)

(vom 12. Februar 2007)[1, 2]

Der Kantonsrat,

nach Einsichtnahme in die Anträge des Regierungsrates vom 9. November 2005[3] und der Kommission für Staat und Gemeinden vom 15. September 2006,

beschliesst:

I. Allgemeine Bestimmungen

§ 1. [1] Dieses Gesetz regelt den Umgang der öffentlichen Organe mit Informationen. — Gegenstand und Zweck

[2] Es bezweckt,

a. das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern sowie die Kontrolle des staatlichen Handelns zu erleichtern,

b. die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Daten bearbeiten.

§ 2.[28] Dieses Gesetz gilt für die öffentlichen Organe. — Geltungsbereich

§ 2 a.[27] [1] Dieses Gesetz gilt nicht für das Verhältnis zwischen dem Kantonsrat und seinen ständigen Kommissionen sowie den Behörden und Anstalten, die seiner Oberaufsicht unterstehen. — Ausnahmen a. Kantonsrat

[2] Soweit der Kantonsrat diesem Gesetz untersteht, stehen der oder dem Beauftragten für den Datenschutz die Befugnisse gemäss § 10 Abs. 2, § 12 a Abs. 1 und 2, § 34 lit. c, d und f sowie §§ 35–36 a nicht zu.

§ 2 b.[27] [1] Bei Gerichtsverfahren sowie Verfahren von Strafverfolgungsbehörden gemäss § 86 Abs. 1 lit. b und c des Gesetzes über die Gerichts- und Behördenorganisation im Zivil- und Strafprozess vom 10. Mai 2010[12] richten sich die Rechte der betroffenen Personen und die Einsichtsrechte Dritter nach den spezialgesetzlichen Bestimmungen. — b. Gerichte und Strafverfolgungsbehörden

[2] Für die Bearbeitung von Personendaten gilt dieses Gesetz, soweit Spezialgesetze keine Regelungen enthalten.

1.7.20 - 109 — 1

Gesetz über die Information und den Datenschutz (IDG) des Kantons Zürich, LS 170.4

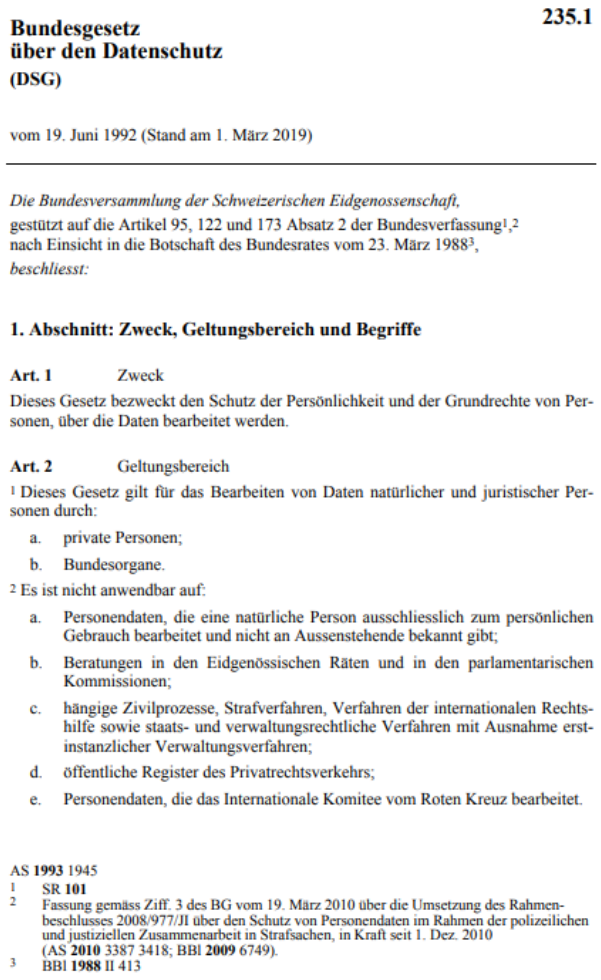
Anwendbar auf kantonale öffentliche Organe, inkl. Gemeinden.

Direktlink: https://www.zh.ch/de/politik-staat/gesetze-beschluesse/gesetzessammlung/zhlex-ls/erlass-170_4-2007_02_12-2008_10_01-109.html

Weitere rechtliche Grundlagen:

- Verordnung über die Information und den Datenschutz (IDV), LS 170.41
- Verordnung über die Informationsverwaltung und –sicherheit (IVSV), LS 170.8

II. Einführung in das Datenschutzrecht - Überblick



Bundesgesetz
über den Datenschutz
(DSG)

235.1

vom 19. Juni 1992 (Stand am 1. März 2019)

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 95, 122 und 173 Absatz 2 der Bundesverfassung[1],[2]
nach Einsicht in die Botschaft des Bundesrates vom 23. März 1988[3],
beschliesst:

1. Abschnitt: Zweck, Geltungsbereich und Begriffe

Art. 1 Zweck

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

Art. 2 Geltungsbereich

[1] Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch:

a. private Personen;
b. Bundesorgane.

[2] Es ist nicht anwendbar auf:

a. Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt;
b. Beratungen in den Eidgenössischen Räten und in den parlamentarischen Kommissionen;
c. hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren;
d. öffentliche Register des Privatrechtsverkehrs;
e. Personendaten, die das Internationale Komitee vom Roten Kreuz bearbeitet.

AS **1993** 1945
1 SR **101**
2 Fassung gemäss Ziff. 3 des BG vom 19. März 2010 über die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, in Kraft seit 1. Dez. 2010 (AS **2010** 3387 3418; BBl **2009** 6749).
3 BBl **1988** II 413

Bundesgesetz über den Datenschutz (DSG)

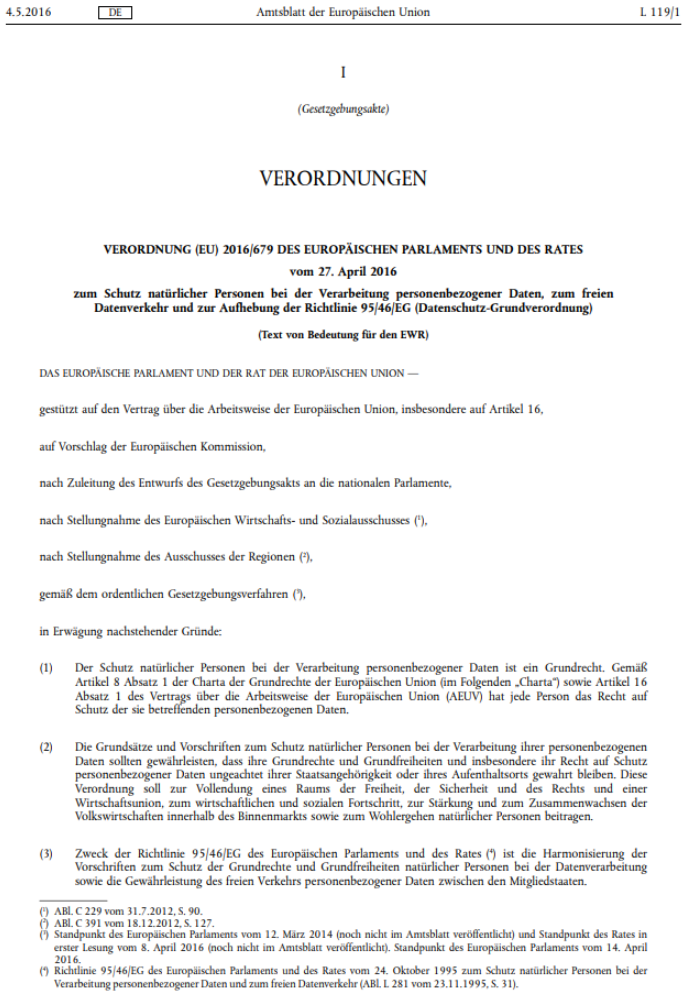
Anwendbar auf die Bundesverwaltung und Private.

Direktlink (aktuell geltende Fassung des DSG):
https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de

Achtung: das revidierte Datenschutzgesetz (revDSG) ist bereits durch das Parlament beschlossen, es muss lediglich noch das Datum des Inkrafttretens festgelegt werden.

Hinweis: derzeit (bis zum 14. Oktober) befindet sich die Verordnung zum Datenschutzgesetz (VDSG) in der Vernehmlassung. **Die Verordnung soll gleichzeitig mit dem revidierten DSG (revDSG) in der zweiten Jahreshälfte 2022 in Kraft treten.** Der Bundesrat wird das genaue Datum zu gegebener Zeit festlegen.

II. Einführung in das Datenschutzrecht - Überblick



4.5.2016 DE Amtsblatt der Europäischen Union L 119/1

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (1),

nach Stellungnahme des Ausschusses der Regionen (2),

gemäß dem ordentlichen Gesetzgebungsverfahren (3),

in Erwägung nachstehender Gründe:

(1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

(3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (4) ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

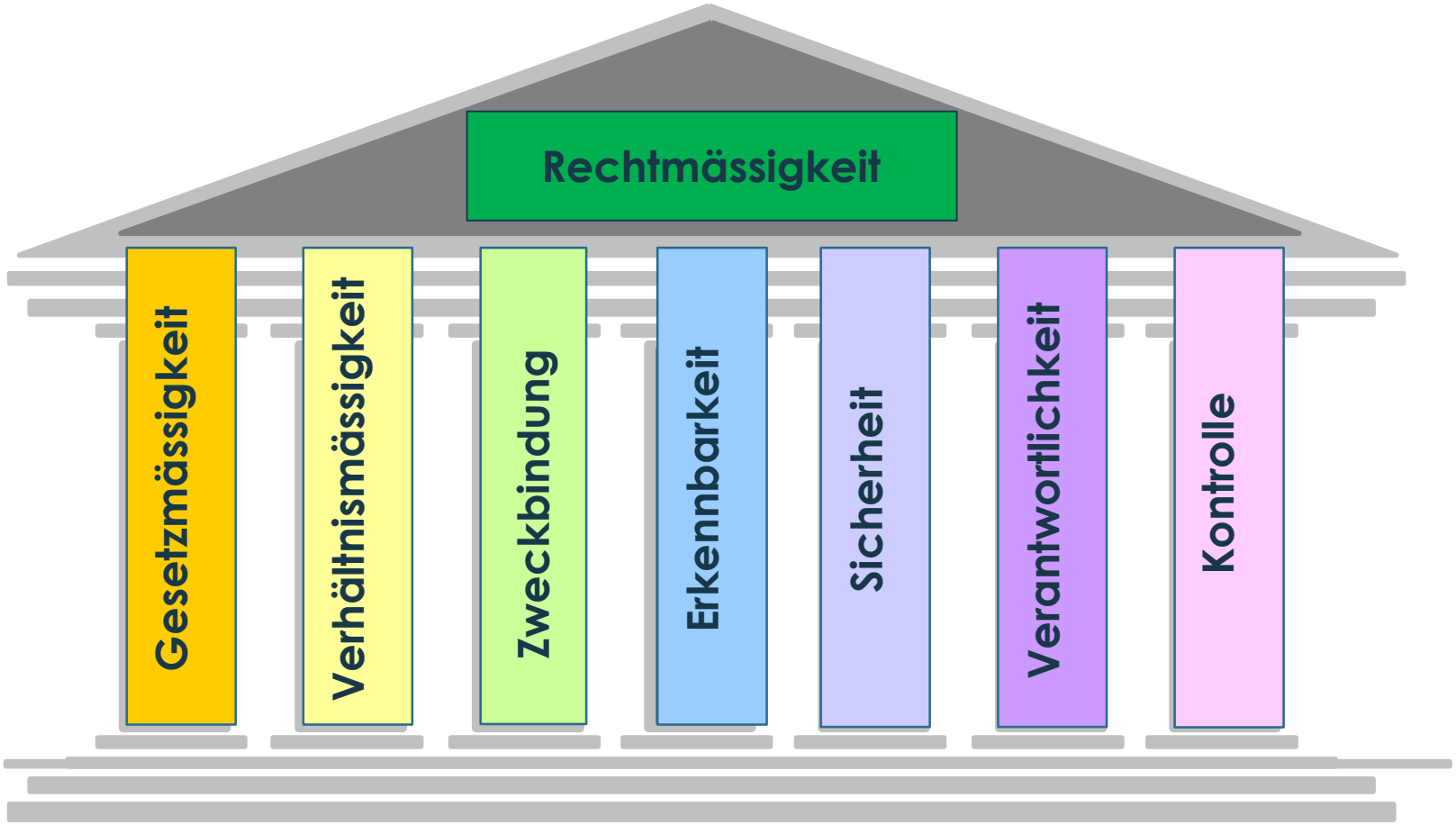
(1) ABl. C 229 vom 31.7.2012, S. 90.
(2) ABl. C 391 vom 18.12.2012, S. 127.
(3) Standpunkt des Europäischen Parlaments vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 14. April 2016.
(4) Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

EU-Datenschutzgrundverordnung (DSGVO/GDPR)

Direktlink: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

II. Einführung in das Datenschutzrecht - Überblick

Grundsätze des Datenschutzes



II. Einführung in das Datenschutzrecht - Überblick

§ 3 Abs. 1 IDG (öffentliche Organe)

1 Öffentliche Organe sind:

a. der Kantonsrat, die Gemeindeparlamente sowie die Gemeindeversammlungen,

b. Behörden und Verwaltungseinheiten des Kantons und der Gemeinden,

c. Organisationen und Personen des öffentlichen und privaten Rechts,
soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind

II. Einführung in das Datenschutzrecht - Überblick

§ 3 Abs. 2 IDG (Informationen)

2 Informationen sind **alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen**, unabhängig von ihrer Darstellungsform und ihrem Informationsträger. Ausgenommen sind Aufzeichnungen, die nicht fertig gestellt oder die ausschliesslich zum persönlichen Gebrauch bestimmt sind.

II. Einführung in das Datenschutzrecht - Überblick

§ 3 Abs. 3 IDG (Personendaten)

3 Personendaten sind Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen.

II. Einführung in das Datenschutzrecht - Überblick

§ 3 Abs. 2 IDG (besondere Personendaten)

4 Besondere Personendaten sind:

a. Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht, **wie Informationen über**

1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen oder Sanktionen.

b. **Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben**.

II. Einführung in das Datenschutzrecht - Überblick

§ 3 Abs. 5 IDG (Bearbeiten)

5 Bearbeiten ist jeder Umgang mit Informationen wie das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben oder Vernichten.

II. Einführung in das Datenschutzrecht - Überblick

§ 3 Abs. 6 IDG (Bekanntgeben)

6 Bekanntgeben ist das Zugänglichmachen von Informationen wie das Einsichtgewähren, Weitergeben oder Veröffentlichen.

II. Einführung in das Datenschutzrecht - Überblick

§ 6 Abs. 1 IDG (Bearbeiten im Auftrag)

1 Das öffentliche Organ kann das Bearbeiten von Informationen Dritten übertragen, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht.

II. Einführung in das Datenschutzrecht - Überblick

Auftragsbearbeitung (Outsourcing), § 6 IDG, § 25 IDV

- **Anwendungsbereich: Auslagerung der Bearbeitung von Informationen an Dritte durch ein öffentliches Organ**

- **Anforderungen des IDG an eine Auftragsbearbeitung:**

  - Kein Entgegenstehen rechtlicher Bestimmungen (wie bspw. Berufs- oder Amtsgeheimnis).
  - Kein Entgegenstehen vertraglicher Bestimmungen (bspw. Klauseln, die ein Outsourcing ausschliessen).
  - Nach § 25 Abs. 1 IDV muss der Vertrag schriftlich geschlossen werden.
  - Es müssen die inhaltlichen Anforderungen nach § 25 Abs. 2 IDV im Vertrag enthalten sein (also u.a. Gegenstand und Umfang der Auftragsbearbeitung, Umgang mit Personendaten, Schutzmassnahmen für die Informationen, usw.), das Grundgerüst der Vertragselemente wird im Leitfaden der Datenschutzbeauftragten präzisiert.
  - Sollte es zusätzlich zu einer Auftragsbearbeitung im Ausland kommen, sind § 19 IDG und § 22 IDV zu beachten.

Vgl. zur Thematik auch das Merkblatt der Datenschutzbeauftragen: Leitfaden Bearbeiten im Auftrag (datenschutz.ch) und die Publikation *Griesinger*, ***Kantonsrechtliche Vorgaben für die Ausgestaltung von Vertragsverhältnissen mit Auftragsverarbeitern für öffentliche Organe des Kantons Zürich***, PinG 2018, 208 ff.

II. Einführung in das Datenschutzrecht - Überblick

§ 19 IDG (Grenzüberschreitender Datentransfer)

An Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen, gibt das öffentliche Organ Personendaten bekannt, wenn

a. im Empfängerstaat ein angemessener Schutz für die Datenübermittlung gewährleistet ist,

b. eine gesetzliche Grundlage dies erlaubt, um bestimmte Interessen der betroffenen Person oder überwiegende öffentliche Interessen zu schützen, **oder**

c. vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen werden.

II. Einführung in das Datenschutzrecht - Überblick

Datenschutzfolgeabschätzung

§ 10 IDG

Das öffentliche Organ bewertet bei einer beabsichtigten Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen (Datenschutz-Folgenabschätzung).

Es unterbreitet eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Grundrechte der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung (Vorabkontrolle).

II. Einführung in das Datenschutzrecht - Überblick

Cloud Computing

Merkblatt DSB: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf

- Ist «Bearbeiten im Auftrag»
- Ausgangspunkt ist eine DSFA: Festhalten
  - Anforderungen an Anbieter
  - Weiterer Inhalt eines Vertrages
  - Cloudspezifische Punkte detailliert regeln
  - Regelmässig kontrollieren
- Öffentliche Organe können Cloud Computing nutzen, wenn
  - Pflichten in Bezug auf Datenschutz wahrnehmen können
  - Pflichten in Bezug auf Informationssicherheit wahrnehmen können
  - Öffentliches Organ bleibt verantwortlich
- Es gibt cloud-spezifische Risiken

II. Einführung in das Datenschutzrecht - Überblick

Drei Schritte

- Risikoanalyse und Anbieterauswahl
- Vertragsgestaltung
- Umsetzung von Massnahmen

II. Einführung in das Datenschutzrecht - Überblick

Risikoanalyse und Anbieterauswahl

- Risikoanalyse im Rahmen der DSFA
- Auswahl des Anbieters mit technischen, organisatorischen und rechtlichen Anforderungen
- Cloud-spezifische Risiken

II. Einführung in das Datenschutzrecht - Überblick

– **Cloudspezifische Risiken:**

- Wahrnehmung der Verantwortung durch beide Parteien
- Anwendung schweizerischen Rechts und Vereinbarung eines schweizerischen Gerichtsstand
- Möglicher Einfluss ausländischer Rechtsordnungen
- Verlust der Kontrolle oder Verunmöglichung der Kontrollpflichten
- Durchsetzbarkeit der Löschungs- und Berichtigungsansprüche
- Gewährleistung eines gleichwertigen Datenschutzniveaus
- Umsetzung der notwendigen IT-Sicherheitsmassnahmen
- Überprüfbarkeit der Abläufe und Prozesse
- Nachvollziehbarkeit der Datenbearbeitungen
- Datenverlust
- Datenmissbrauch
- Eingeschränkte Verfügbarkeit der Dienste
- Portabilität und Interoperabilität

II. Einführung in das Datenschutzrecht - Überblick

Vertragsgestaltung und Umsetzung

- Verweis auf Merkblatt DSB: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf

- Insbesondere: Gleichwertiges Datenschutzniveau (§ 19 IDG)

DSB betr. Auslagerung ins Ausland unter Berücksichtigung Geheimnispflichten: Merkblatt siehe https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/weitere-themen/outsourcing/verschluesselung_der_datenablage_im_rahmen_der_auslagerung.pdf

II. Einführung in das Datenschutzrecht - Überblick

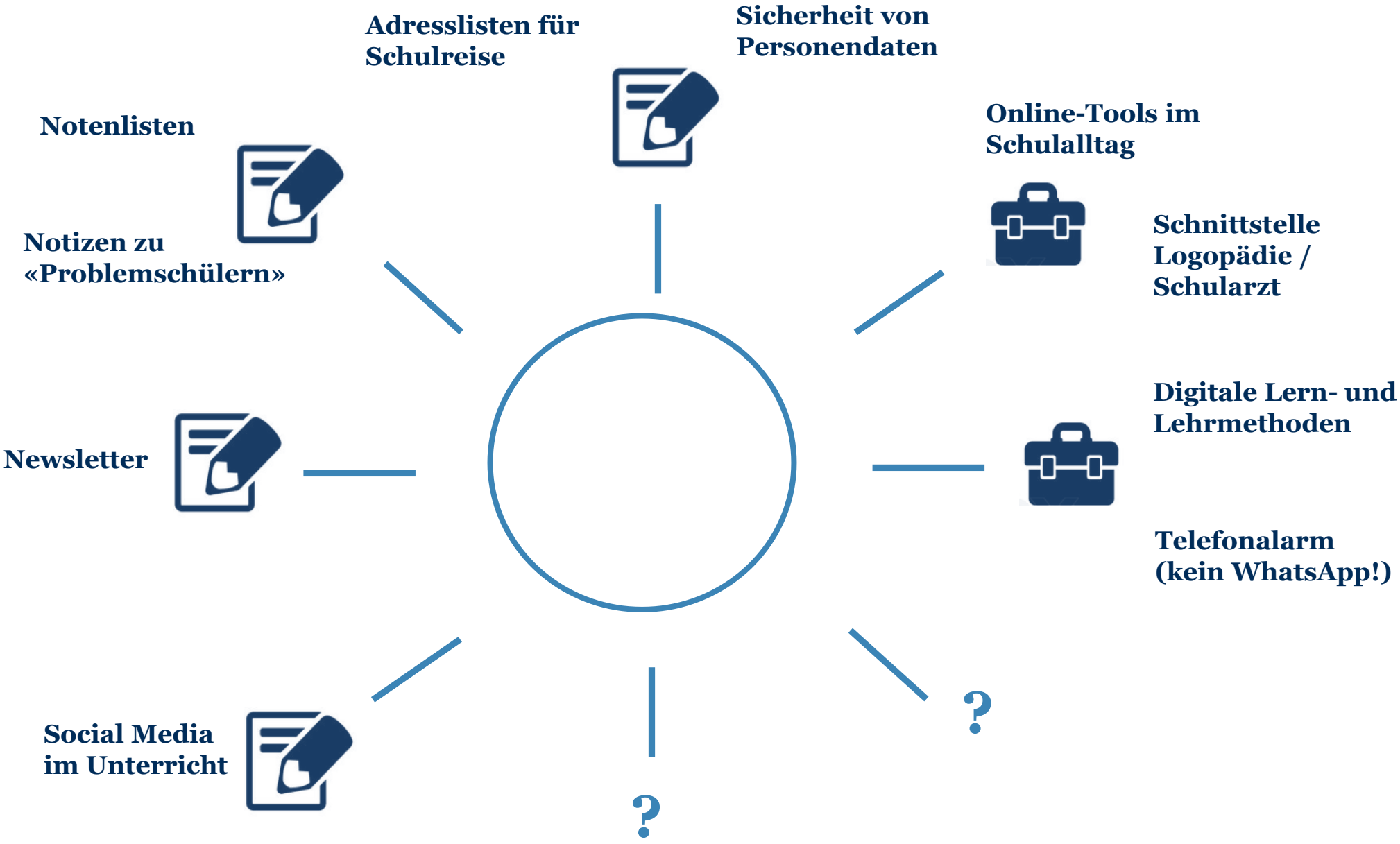
Konkrete Beispiele

- Beispiel: Microsoft 365: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/leitfaeden/leitfaden_microsoft_365_im_bildungsbereich.pdf

- Produkte für Distance Learning
  - Liste «Digitale Zusammenarbeit» bei DSB: https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/digitale-zusammenarbeit
  - Unterschiede zwischen allgemein zugelassen und «nur während der Corona-Krise» zugelassen

II. Einführung in das Datenschutzrecht – Datenschutz und Schulbetrieb

II. Einführung in das Datenschutzrecht – Datenschutz und Datensicherheit im Schulbetrieb



II. Einführung in das Datenschutzrecht – Umsetzungsmassnahmen Datensicherheit

Zentrale Vorschrift im Zusammenspiel von Datenschutz und Datensicherheit ist § 7 IDG-ZH (Gesetz über die Information und den Datenschutz):

§ 7 IDG (Informationssicherheit)

1 Das öffentliche Organ schützt Informationen durch angemessene organisatorische und technische Massnahmen.

2 Die Massnahmen richten sich nach den folgenden Schutzzielen:

a. Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen,
b. Informationen müssen richtig und vollständig sein,
c. Informationen müssen bei Bedarf vorhanden sein,
d. Informationsbearbeitungen müssen einer Person zugerechnet werden können,
e. Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

3 Die zu treffenden Massnahmen richten sich nach der Art der Information, nach Art und Zweck der Verwendung und nach dem jeweiligen Stand der Technik.

§ 7 Abs. 2 IDG – zentrale Schutzziele / Leitlinien

Vertraulichkeit **Integrität** **Verfügbarkeit**

§ 7 Abs. 2 IDG – zentrale Schutzziele / Leitlinien

Vertraulichkeit: Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen

Integrität: Informationen müssen richtig und vollständig sein

Verfügbarkeit: Informationen müssen bei Bedarf vorhanden sein

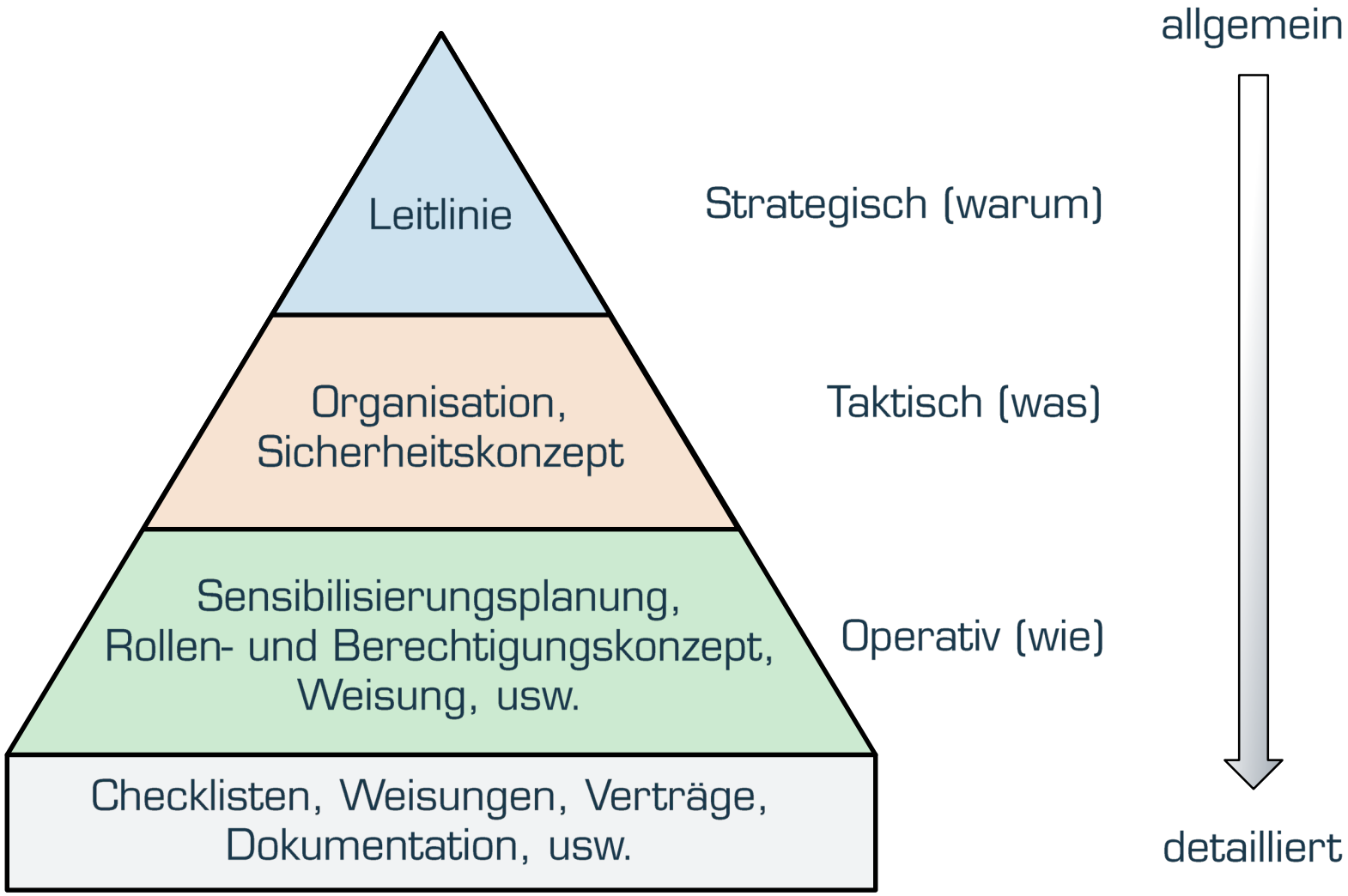
II. Einführung in das Datenschutzrecht – Umsetzungsmassnahmen Datensicherheit

Wesentliche Umsetzungserfordernisse und Umsetzungsmassnahmen werden im **Leitfaden der Datenschutzbeauftragten des Kantons Zürich zur Informationssicherheit** in Volksschulen dargestellt.

Zur konkreten Umsetzung der zentralen Anforderungen an die Datensicherheit werden unterschiedliche **Vorlagen-Dokumente** von der Datenschutzbeauftragten bereit gehalten.

Wir möchten Ihnen im folgenden Abschnitt einen Überblick zu diesen Anforderungen und Dokumenten geben und dabei insbesondere die Bereiche «**Sicherheitsstrategie**», «**Organisationsstruktur**», «**Schutzbedarfsermittlung**» und «**Sicherheits-massnahmen**» vertiefen.

II. Einführung in das Datenschutzrecht – Dokumente Datensicherheit



Kaffeepause

Kaffeepause von

14.45 bis 15.15 Uhr

III. Informationssicherheit

III. Überblick Informationssicherheit
1. Thematische Übersicht («um was geht es»)
2. Zielsetzung der Informationssicherheit («wo wird es relevant»)
3. Übersicht Dokumente («was ist nun zu tun»)
4. Anforderungen an die Informationssicherheit («was ist nun zu tun»)
5. Aufrechterhaltung der Standards der Informationssicherheit («was ist nun zu tun»)

III. Informationssicherheit - Thematische Übersicht

Der Leitfaden zur Informationssicherheit hilft bei der **Einführung, Umsetzung und Pflege einer nachhaltigen Informationssicherheit**.

Er enthält eine **Übersicht** der vom Gesetz über die Information und den Datenschutz (IDG) **geforderten Massnahmen zur Informationssicherheit** sowie eine Einführung, wie diese umgesetzt werden.

Im Weiteren sind von der Datenschutzbeauftragten (DSB) zur Verfügung gestellten **Anleitungen und Vorlagen im Leitfaden hinterlegt** bzw. verlinkt.

III. Informationssicherheit – Zielsetzung

Eine datenbearbeitende Stelle hat die **angemessenen Massnahmen auf der organisatorischen und technischen Ebene** zu treffen.

Das Schutzziel ist, **Personendaten gegen unbefugte Bearbeitungsvorgänge zu schützen**. Bearbeiten ist dabei jeglicher Umgang mit Personendaten.

Die zu treffenden **Massnahmen** richten sich **nach der Art der Information, nach Art und Zweck der Verwendung** und nach dem **jeweiligen Stand der Technik**.

III. Informationssicherheit – Übersicht Dokumente

Für die Erstellung und Einführung der nötigen Leitlinien, Weisungen und Konzepte stehen folgende Dokumente zur Verfügung.

Dokumente	**Thema**
Leitfaden	Informationssicherheit in Volksschulen
Anleitungen	Sensibilisierung der Mitarbeitenden für Informationssicherheit in Volksschulen
Vorlagen	Erklärung zur Informationssicherheit in Volksschulen
	Leitlinie zur Informationssicherheit in Volksschulen
	Rollen- und Berechtigungskonzept in Volksschulen
	Schutzbedarfsfeststellung Fachanwendungen in Volksschulen
	Weisung zur Informationssicherheit in Volksschulen
Checklisten	Minimummassnahmenkatalog
Glossar / Abkürzungsverzeichnis	Glossar und Abkürzungen Informationssicherheit

Die Datenschutzbeauftragte stellt unterschiedliche Dokumente zu spezifischen Themen zur Verfügung.

III. Informationssicherheit - Anforderungen

4. Anforderungen an die Informationssicherheit
a. Sicherheitsstrategie
b. Organisationsstruktur
c. Ermittlung Schutzbedarf
d. Sicherheitsmassnahmen

III. Informationssicherheit - Anforderungen

Sicherheitsstrategie

Die Sicherheitsstrategie, das angestrebte Sicherheitsniveau sowie die für die Volksschule gültigen Sicherheitsziele müssen definiert und festgehalten werden.

Als Vorlage wird die Leitlinie zur Informationssicherheit in Volksschulen zur Verfügung gestellt: vorlage_leitlinie_informationssicherheit_volksschule.docx (live.com)

Was ist zu tun:

1. Layout der Vorlage Leitlinie zur Informationssicherheit an das eigene Corporate Design anpassen
2. Inhalt überprüfen und ergänzen
3. Leitlinie durch einen Beschluss [des verantwortlichen Gremiums] in Kraft setzen
4. Leitlinie allen Mitarbeitenden kommunizieren und an einem für diese zugänglichen Ort publizieren

III. Informationssicherheit - Anforderungen

Organisationsstruktur

Um das von der Schule angestrebte Sicherheitsniveau zu erreichen, muss ein **Informationssicherheitsprozess definiert, dokumentiert und umgesetzt** werden. Zu diesem Zweck müssen eine **Organisationsstruktur** aufgebaut, die **Rollen festgelegt** und den **Rollen die Aufgaben zugeordnet** werden.

Als Vorlage wird eine mögliche Regelung zur Verfügung gestellt:
vorlage_leitlinie_informationssicherheit_volksschule.docx (live.com)

Was ist zu tun:

1. Rollenträgerinnen und -träger definieren und kommunizieren
2. Aufgaben in die Stellenbeschreibungen integrieren
3. Ressourcen den Rollenträgerinnen und -trägern zuweisen
4. Ausbildungsmassnahmen durchführen

III. Informationssicherheit - Anforderungen

Ermittlung Schutzbedarf

Hintergrund: § 12 Verordnung über Informationsverwaltung und –sicherheit (IVSV: 170.8_3.9.19_107.fm (zh.ch)) verlangt, die **Risiken sowie** den **Schutzbedarf** der verwalteten Informationen **festzustellen**. Dies als **Grundlage für** einen Plan, in welchem **angemessene Massnahmen** zu deren Schutz festgelegt werden. Dabei sollen die Schutzziele von § 7 IDG (siehe dazu oben) erreicht werden.

Es wird eine «Vorlage Schutzbedarfsfeststellung Fachanwendungen an Volksschulen» zur Verfügung gestellt.

Was ist zu tun:

1. Liste der Fachanwendungen erstellen
2. Anwendungsverantwortlichen bestimmen
3. Schutzbedarf der Fachanwendungen (Vertraulichkeit/Integrität/Verfügbarkeit) festlegen

III. Informationssicherheit - Anforderungen

Ermittlung Schutzbedarf

Schulen verfügen über diverse IT **Fachanwendungen**, die der Erfüllung oder Unterstützung diverser Aufgaben dienen.
Diese Anwendungen sind zu **erheben** und zu **inventarisieren**.

Darüber hinaus erscheint es uns (aus genereller datenschutzrechtlicher Sicht) hilfreich, auch allfällige andere Verarbeitungsprozesse sowie die genutzte IT Infrastruktur generell zu erheben.

Was ist zu tun:

1. Liste der Fachanwendungen erstellen

III. Informationssicherheit - Anforderungen

Ermittlung Schutzbedarf

Gestützt auf die Liste der Fachanwendungen sollte für jede dieser Anwendungen festgelegt werden, wer für ihre Sicherheit verantwortlich ist.

Verantwortliche können intern oder (zusätzlich) extern, wie bspw. Auftragnehmende sein. Gerade bei externen Verantwortlichen ist der Datenstandort relevant.

Dessen Aufgaben können in Leitlinie beschrieben werden.

Was ist zu tun:

1. Interne Verantwortliche bestimmen (und auch dokumentieren)
2. Externe Verantwortliche dokumentieren (bspw. Auftragnehmende)
3. Datenstandort ermitteln und dokumentieren (intern/extern; falls extern: wo?)

III. Informationssicherheit - Anforderungen

Ermittlung Schutzbedarf

Gestützt auf die Liste der Fachanwendungen sollte für jede dieser Anwendungen der Schutzbedarf gemäss der Vorlage bestimmt werden

Verschiedene Kategorien gemäss Beispiel-Liste

Was ist zu tun:

1. Schutzbedarfskategorien ermitteln, überprüfen und allenfalls ergänzen
2. Feststellung Schutzbedarf der einzelnen Anwendungen betr. Vertraulichkeit, Verfügbarkeit und Integrität (anhand Schutzbedarfskategorien)
3. Überprüfen und anpassen

III. Informationssicherheit - Anforderungen

Sicherheitsmassnahmen planen und umsetzen

Hintergrund: Für die Informationssicherheit sind die angemessenen Massnahmen zu planen und umzusetzen

Es steht ein Minimummassnahmenkatalog zur Verfügung. Dieser erscheint uns sehr umfangreich …

Was ist zu tun:

1. Sicherheitsmassnahmen den Verantwortlichen zuweisen (verantwortliche Mitarbeitende oder Auftragnehmende bestimmen und dokumentieren
2. Status Massnahmen bestimmen und dokumentieren
3. Gap-Analyse
4. Umsetzung planen; mit Termin, Priorität und Kosten
5. (Revision planen)

III. Informationssicherheit - Anforderungen

Sicherheitsmassnahmen planen und umsetzen

Hintergrund: Bei der Umsetzung von Sicherheitsmassnahmen sind gemäss dem Leitfaden die nachfolgend aufgeführten Massnahmen prioritär zu behandeln.

Wir werden uns deshalb auf diese (als prioritär) konzentrieren …

Was ist zu tun:

1. Weisungen für die Mitarbeitenden erstellen
2. Sensibilisierung der Mitarbeitenden planen
3. Rollen- und Berechtigungskonzept erstellen

III. Informationssicherheit - Aufrechterhaltung Standards

Um die Sicherheitsstandards aufrecht zu erhalten, werden folgende Massnahmen empfohlen (Informationssicherheit | DSB Kanton Zürich (datenschutz.ch)):

- **Weisungen für Mitarbeitende, Vorlage:**
  vorlage_weisung_zur_informationssicherheit_in_volksschulen.docx (live.com)
- **Erklärung zur Informationssicherheit, Vorlage:**
  vorlage_erklaerung_informationssicherheit_volksschulen.docx (live.com)
- **Sensibilisierung der Mitarbeitenden, Vorlage:** Anleitung Sensibilisierung der Mitarbeitenden für Informationssicherheit in Volksschulen (zh.ch)
- **Rollen- und Berechtigungskonzept, Vorlage:**
  beispiel_rollen_und_berechtigungskonzept_in_volksschulen.docx (live.com)
- **Regelmässige Überprüfung der Umsetzung der Massnahmen**

Aufgabe(n) und Ausblick für Tag 2

Bitte durch lesen Sie die besprochenen Dokumente durch und formulieren Sie allfällige Fragen.

- ✓ **Vorlage Weisung zur Informationssicherheit in Volksschulen**
- ✓ **Vorlage Leitlinie zur Informationssicherheit in Volksschulen**
- ✓ **Vorlage Erklärung über die Nutzung von Internet und E-Mail sowie zur Informatiossicherheit in Volksschulen**
- ✓ **Vorlage Sensibilisierung der Mitarbeitenden für Informationssicherheit**
- ✓ **Vorlage Rollen- und Berechtigungskonzept in Volksschulen**

Soweit möglich, bitten wir um vorgängige Zusendung Ihrer Fragen vor dem kommenden Termin.

Vielen Dank.

Weitere Themen

- Einsatz von DropBox
- Einsatz von WhatsApp
- Einsatz von Quizlet
- Einsatz / Verwendung von TikTok
- Einsatz von Google-Tools