HÄRTING

Datensicherheit und Meldepflichten nach nDSG und ISG im Beschaffungsprozess

RAin lic. iur. Nicole Beranek Zanon

ÜBERSICHT

I. Einordnung

I. EINORDNUNG: ÜBERBLICK

Inkrafttreten am 01.09.2023:

- DSG + DSV
- ISG + ISV (ISG noch ohne Meldepflicht)

Quelle: P042 - Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept), vom 19. Dezember 2013 (Stand 1. April 2021) abrufbar unter file://dc2.first365.net/users$/5%20GB/beranek_11918/Downloads/P042-ISDS_Konzept_V4-4-d%20(1).pdf, (Stand 20.08.2023

I: EINORDNUNG: SCHUTZOBJEKT

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

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 beim Bund
(Informationssicherheitsgesetz, ISG)

vom 18. Dezember 2020

Art. 1 Zweck

[1] Dieses Gesetz soll die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten.

[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.

II. Datensicherheit gem. nDSG + DSV

1. Rechtsgrundlagen DSG

1. RECHTSGRUNDLAGEN DSG: TERMINOLOGIE

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 5 Begriffe

In diesem Gesetz bedeuten:

h. *Verletzung der Datensicherheit:* eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;

j. *Verantwortlicher:* private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;

k. *Auftragsbearbeiter:* private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

1. RECHTSGRUNDLAGEN DSG: DATENSICHERHEIT

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 8 Datensicherheit

1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

2 Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

- Abs. 2
  - Möglichkeit der Vermeidung zwingend! → fehlt in den meisten TOM's!
  - Ungeeignete Massnahmen sind damit nicht tauglich!
- Abs. 3 Mindestanforderungen gemäss DSV

1. RECHTSGRUNDLAGEN DSG: WESHALB?

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 61 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft, die vorsätzlich:

a. unter Verstoss gegen Artikel 16 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 17 erfüllt sind, Personendaten ins Ausland bekanntgeben;

b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 9 Absätze 1 und 2 erfüllt sind;

c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach

Art. 62 Verletzung der beruflichen Schweigepflicht

1 Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.

2 Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser Kenntnis erlangt hat.

3 Das Offenbaren geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.

1. RECHTSGRUNDLAGEN DSG: KONSEQUENZEN IM BESCHAFFUNGSPROZESS

- Klare Definition der Rollen (in Anlehnung an DSGVO-Begrifflichkeiten)
- Keine eigenständige Definition der Verletzung der Datensicherheit in Verträge aufnehmen
- Mindestvorgaben DSV treffen auch den Auftragsverarbeiter
- Vorsatz ist auch schon bei Eventualvorsatz («in Kauf nehmen») erfüllt!

2. Mindestanforderungen nach DSV

2. MINDESTANFORDERUNGEN DSV: GRUNDSÄTZE

Art. 1 Grundsätze

1 Zur Gewährleistung einer angemessenen Datensicherheit müssen der Verantwortliche und der Auftragsbearbeiter den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen.

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

1. Abschnitt: Datensicherheit

2 Der Schutzbedarf der Personendaten wird nach den folgenden Kriterien beurteilt:

a. Art der bearbeiteten Daten;

b. Zweck, Art, Umfang und Umstände der Bearbeitung.

3 Das Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person wird nach den folgenden Kriterien beurteilt:

a. Ursachen des Risikos;

b. hauptsächliche Gefahren;

c. ergriffene oder vorgesehene Massnahmen, um das Risiko zu verringern;

d. Wahrscheinlichkeit und Schwere einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen.

4 Bei der Festlegung der technischen und organisatorischen Massnahmen werden zudem die folgenden Kriterien berücksichtigt:

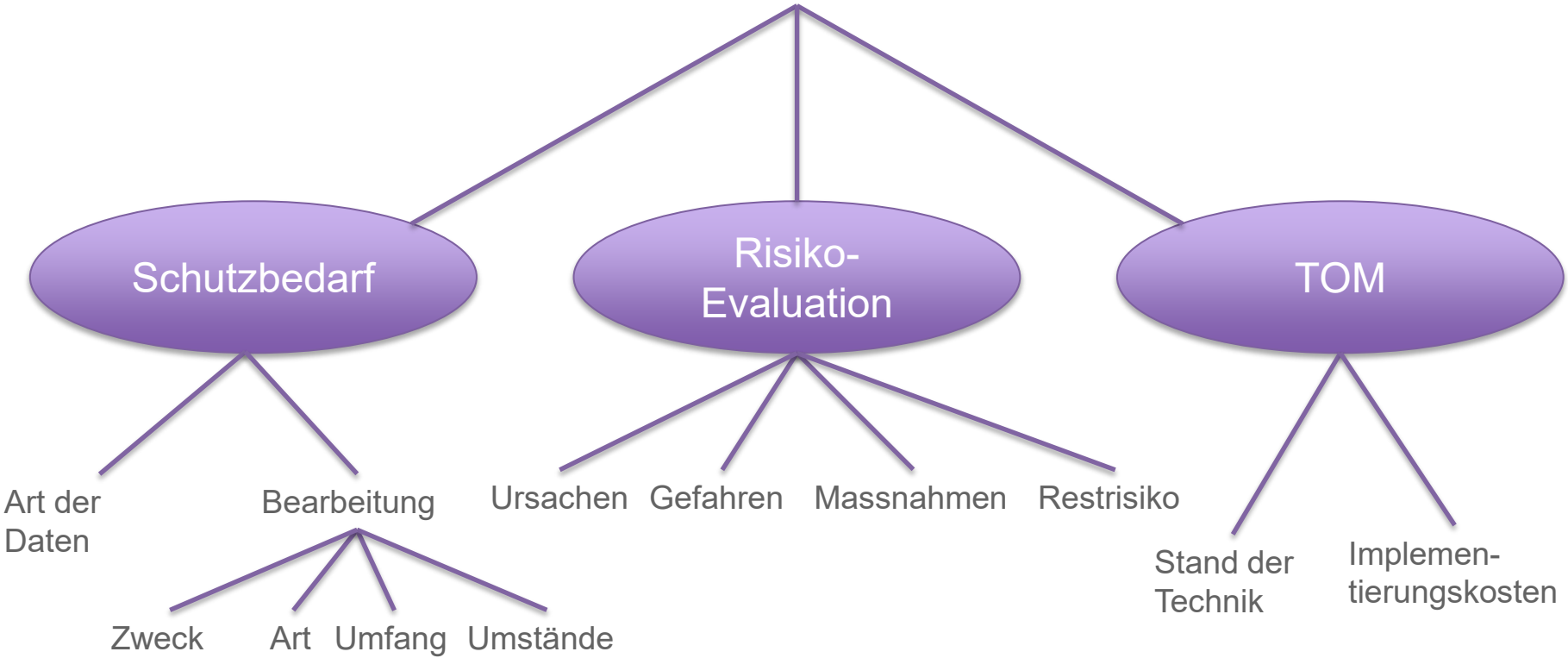
a. Stand der Technik;

b. Implementierungskosten.

5 Der Schutzbedarf der Personendaten, das Risiko und die technischen und organisatorischen Massnahmen sind über die gesamte Bearbeitungsdauer hinweg zu überprüfen. Die Massnahmen sind nötigenfalls anzupassen.

Kriterien gestützt auf geltendes Recht

2. MINDESTANFORDERUNGEN DSV: ÜBERBLICK



2. MINDESTANFORDERUNGEN DSV: KONSEQUENZEN IM BESCHAFFUNGSPROZESS

3. Ziele und Massnahmen

3. ZIELE UND MASSNAHMEN: ZIEL VERMEIDUNG VERLETZUNG DER DATENSICHERHEIT

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 8 Datensicherheit

[1] Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

[2] Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

DSV!

[3] Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

3. ZIELE UND MASSNAHMEN: MASSNAHMEN (1)

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

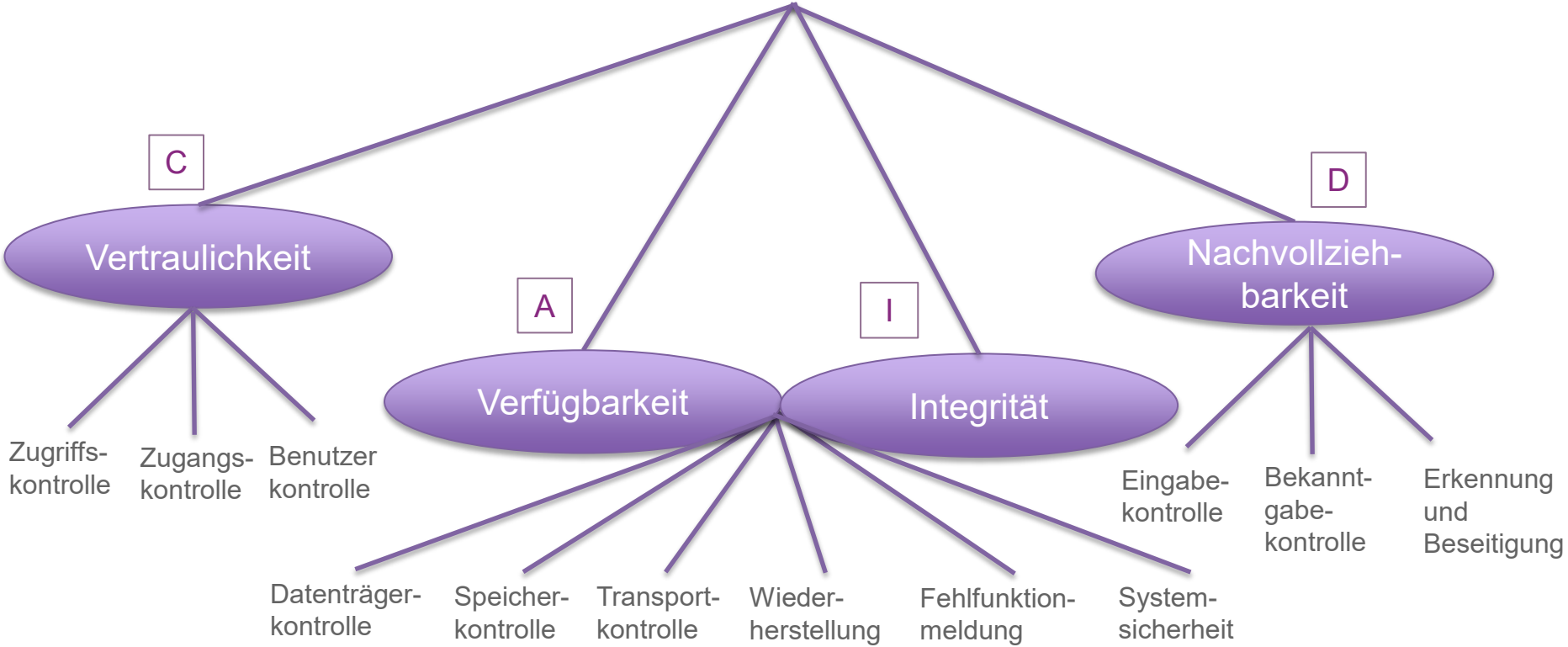
1. Abschnitt: Datensicherheit

Art. 2 Ziele

Der Verantwortliche und der Auftragsbearbeiter müssen technische und organisatorische Massnahmen treffen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechend:

a. nur Berechtigten zugänglich sind (Vertraulichkeit); C
b. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit); A
c. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität); I
d. nachvollziehbar bearbeitet werden (Nachvollziehbarkeit). D

3. ZIELE UND MASSNAHMEN: MASSNAHMEN (2)



4. Protokollierung

4. PROTOKOLLIERUNG

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

1. Abschnitt: Datensicherheit

Art. 4 Protokollierung

[1] Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der private Verantwortliche und sein privater Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Eine Protokollierung muss insbesondere dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.

[2] Das verantwortliche Bundesorgan und sein Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten.

[3] Bei Personendaten, welche allgemein öffentlich zugänglich sind, sind zumindest das Speichern, Verändern, Löschen und Vernichten der Daten zu protokollieren.

[4] Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

[5] Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

Voraussetzungen für die Pflicht zur Protokollierung

öffentlich zugängliche Personendaten

Umfang

Aufbewahrung

5. Bearbeitungsreglement

5. BEARBEITUNGSREGLEMENT: RECHTSGRUNDLAGE

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

1. Abschnitt: Datensicherheit

Art. 6 Bearbeitungsreglement von Bundesorganen

[1] Das verantwortliche Bundesorgan und sein Auftragsbearbeiter erstellen ein Bearbeitungsreglement für automatisierte Bearbeitungen, wenn sie:

a. besonders schützenswerte Personendaten bearbeiten;
b. ein Profiling durchführen;
c. nach Artikel 34 Absatz 2 Buchstabe c DSG Personendaten bearbeiten;
d. Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen Personendaten zugänglich machen;
e. Datenbestände miteinander verknüpfen; oder
f. mit anderen Bundesorganen zusammen ein Informationssystem betreiben oder Datenbestände bewirtschaften.

[2] Das Reglement muss insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten.

[3] Das verantwortliche Bundesorgan und sein Auftragsbearbeiter müssen das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater zur Verfügung stellen.

5. BEARBEITUNGSREGLEMENT: MUSTER

- Muster beim NCSC: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/vorgaben/prozesse/p042/P042-Hi04-Bearbeitungsreglement_V2-1-d.docx.download.docx/P042-Hi04-Bearbeitungsreglement_V2-1-d.docx
- Im Rahmen der Beschaffung: Unterstützungspflicht des Auftragsverarbeiter zur Erarbeitung des Bearbeitungsreglementes

ZUSAMMENFASSUNG: DATENSICHERHEIT NACH DSG UND DSV

- Schutzbedarf muss vor der Ausschreibung klar sein und als Eignungskriterium definiert werden.
- Zweck ist initial zu definieren und setzt den Rahmen der Bearbeitung .
- Risikobeurteilung ist vor Vertragsabschluss mit dem Auftragnehmer vorzunehmen.
- Bereitschaft ein Restrisiko zu übernehmen, sollte zuvor strategisch festgelegt werden.
- Wirksame Kontrollen und Kontroll-Intervalle sind festzulegen.
- Kosten für den Schutzbedarf ist nur für den Mehrbedarf durch den Verantwortlichen zu tragen.
- Die technischen und organisatorischen Massnahmen sind für die Ausschreibung als Eignungkriterien zu definieren.
- IT-Security-Assessement muss vor Vertragsabschluss.
- Protokollierung ist festzulegen und sicherzustellen, dass es getrennt aufbewahrt wird unter erweitertem Schutz
- Bearbeitungsreglement ist zusammen mit allen Massnahmen regelmässig anzupassen hinsichtlich sich verändernder Risiken und Technologie

III. Informationssicherheit gem. ISG

III. INFORMATIONSSICHERHEIT NACH ISG: RECHTSGRUNDLAGE

Bundesgesetz
über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

vom 18. Dezember 2020

Art. 2 Verpflichtete Behörden und Organisationen

1 Dieses Gesetz gilt für die nachstehenden Behörden (verpflichtete Behörden):

a. die Bundesversammlung;
b. den Bundesrat;
c. die eidgenössischen Gerichte;
d. die Bundesanwaltschaft und die Aufsichtsbehörde über die Bundesanwaltschaft;
e. die Schweizerische Nationalbank.

2 Es gilt für die nachstehenden Organisationen (verpflichtete Organisationen):

a. die Parlamentsdienste;
b. die Bundesverwaltung;
c. die Verwaltungen der eidgenössischen Gerichte;
d. die Armee;
e. Organisationen nach Artikel 2 Absatz 4 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[3] (RVOG) für ihre Verwaltungsaufgaben.

Art. 9 Zusammenarbeit mit Dritten

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.

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

Art. 3 Geltung für die Kantone

1 Für die Kantone gelten nur die Bestimmungen:

a. über klassifizierte Informationen, soweit sie klassifizierte Informationen des Bundes bearbeiten; und
b. über die Sicherheit beim Einsatz von Informatikmitteln, soweit sie auf Informatikmittel des Bundes zugreifen.

2 Diese Bestimmungen gelten nicht, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten.

III. INFORMATONSSICHERHEIT NACH ISG: ISMS

Informationssicherheits-Management-System (ISMS)

- Beurteilung Schutzbedarf (Art. 6 ISG)
- Ggf. Klassifizierung der Informationen (Art. 11-15 ISG)
- Risikomanagement (Art. 8 ISG)
- Sicherheitsverfahren und Sicherheitsmassnahmen (Art. 16-19 ISG)
- Personeller und physischer Schutz (Art. 20-23 ISG)

III. INFORMATIONSSICHERHEIT NACH ISG: INFORMATIONSSICHERHEIT

- Informationssicherheit ist breiter als Datenschutz
- ISO 27001/2 auch hier Grundlage
- Detailliertere Anforderungen, dabei aber die verschiedenen Ziele der beiden Gesetze nicht vergessen.
- Idem Datenschutz

III. INFORMATIONSSICHERHEIT NACH ISG: HILFSMITTEL DES NCSC

ISDS-Konzept: Vorlage

Als Vorlage für die Erstellung eines ISDS-Konzeptes steht das Dokument ISDS-Konzept zur Verfügung.

P042 - Hi01: ISDS-Konzept - Version 4.4 (DOCX, 355 kB, 23.09.2021)

Risikoanalyse

Die Risikoanalyse ist eine Beschreibung der relevanten Risikofaktoren (Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit) und eine Auflistung und Bewertung der Risiken. Sie zeigt ein Bild über das vorhandene Risikopotential des untersuchten Systems auf.

P042 - Hi02: Detaillierte Risikoanalyse zum ISDS-Konzept - Version 4.2 (XLSX, 97 kB, 19.04.2021)

Notfallkonzept

Das Notfallkonzept beschreibt die Notfallplanung und Katastrophenvorsorge, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.

P042 - Hi03: Notfallkonzept - Version 3.1 (DOCX, 336 kB, 30.03.2022)

Bearbeitungsreglement

Das Bearbeitungsreglement sorgt für die notwendige Transparenz im Umfeld der Systementwicklung und der Datenbearbeitung.

P042 - Hi04: Bearbeitungsreglement - Version 2.1 (DOCX, 74 kB, 06.12.2020)

Abrufbar unter https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html

IV. Meldepflichten

1. Meldepflichten nach DSG

1. MELDEPFLICHTEN DSG: RECHTSGRUNDLAGEN

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 24 Meldung von Verletzungen der Datensicherheit

[1] Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

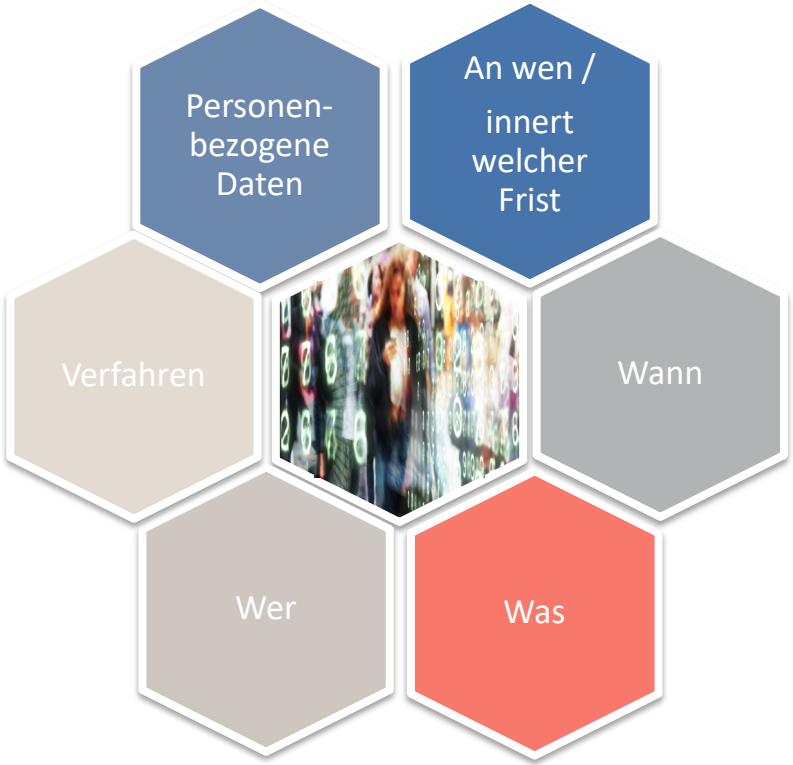
[2] In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

[3] Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

[4] Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

Datensicherheitsverletzung liegt vor, wenn aufgrund einer Sicherheitsverletzung unbeabsichtigt oder widerrechtlich Personendaten verlorengehen, gelöscht, oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden

1 MELDEPFLICHTEN DSG: VORGEHEN



2. Meldepflichten nach ISG de lege lata

2. MELDEPFLICHT NACH ISG DE LEGE LATA: RECHTSGRUNDLAGEN

Art. 10 Vorgehen bei Verletzungen der Informationssicherheit

[1] Die verpflichteten Behörden und Organisationen sorgen dafür, dass Verletzungen der Informationssicherheit rasch erkannt, deren Ursachen abgeklärt und allfällige Auswirkungen minimiert werden.

[2] Die verpflichteten Behörden sorgen dafür, dass für allfällige schwerwiegende Verletzungen der Informationssicherheit, welche die Erfüllung unverzichtbarer Aufgaben des Bundes gefährden können, Vorsorgeplanungen erstellt und entsprechende Übungen durchgeführt werden.

Bundesgesetz
über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

vom 18. Dezember 2020

Art. 73b *Meldungen*

[1] Das NCSC nimmt Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen. Die Meldungen können anonym erfolgen.

[2] Das NCSC analysiert die Meldungen bezüglich ihrer Bedeutung für den Schutz der Schweiz vor Cyberbedrohungen. Es gibt auf Wunsch eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind.

[3] Erhält das NCSC Kenntnis von einer Schwachstelle, so informiert es umgehend die Herstellerin der betroffenen Hard- oder Software und setzt ihr zur Behebung der Schwachstelle eine angemessene Frist. Es weist ihn darauf hin, dass eine Missachtung beschaffungsrechtlich sanktioniert werden kann (Art. 44 Abs. 1 Bst. f[bis] des Bundesgesetzes vom 21. Juni 2019[5] über das öffentliche Beschaffungswesen) und dass das NCSC nach Fristablauf die Schwachstelle gemäss Artikel 73*c* Absatz 2 veröffentlichen kann.

→ Vertragliche oder gesetzliche Geheimhaltungsverpflichtungen sind zu beachten!!!

2. MELDEPFLICHT NACH ISG DE LEGE LATA: PFLICHTIGE

Bundesgesetz
über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

vom 18. Dezember 2020

Art. 74a *Grundsätze*

[1] Behörden und Organisationen nach Artikel 74*b* müssen dafür sorgen, dass dem NCSC Cyberangriffe auf ihre Informatikmittel gemeldet werden.

[2] Das NCSC erteilt interessierten Behörden und Organisationen Auskunft darüber, ob sie der Meldepflicht unterstellt sind und erlässt auf Antrag eine Verfügung über die Unterstellung unter die Meldepflicht.

Art. 74b *Meldepflichtige Behörden und Organisationen*

[1] Die Meldepflicht gilt für: […]

p.m.

Art. 5 Begriffe

In diesem Gesetz bedeuten:

c. *kritische Infrastrukturen:* Trinkwasser- und Energieversorgung, Informations-, Kommunikations- und Transportinfrastrukturen sowie weitere Prozesse, Systeme und Einrichtungen, die essenziell für das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung sind.

2. MELDEPFLICHT NACH ISG DE LEGE LATA: CYBERANGRIFF UND MELDEFRIST

Bundesgesetz
über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

vom 18. Dezember 2020

Art. 74d *Zu meldende Cyberangriffe*

Ein Cyberangriff muss gemeldet werden, wenn er:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet;

b. zu einer Manipulation oder zu einem Abfluss von Informationen geführt hat;

c. über einen längeren Zeitraum unentdeckt blieb, insbesondere wenn Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde; oder

d. mit Erpressung, Drohung oder Nötigung verbunden ist.

Art. 74e *Frist und Inhalt der Meldung*

[1] Die Meldung muss innert 24 Stunden nach der Entdeckung des Cyberangriffs erfolgen.

[2] Sie muss Informationen zur meldepflichtigen Behörde oder Organisation, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und, soweit bekannt, zum geplanten weiteren Vorgehen enthalten.

2. MELDEPFLICHT NACH ISG DE LEGE LATA: VERLETZUNG DER MELDEPFLICHT

Bundesgesetz
über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

vom 18. Dezember 2020

Art. 74g *Verletzung der Meldepflicht*

[1] Bestehen Anzeichen für eine Verletzung der Meldepflicht, so informiert das NCSC die meldepflichtige Behörde oder Organisation darüber und setzt ihr eine angemessene Frist, um der Meldepflicht nachzukommen.

[2] Kommt die meldepflichtige Behörde oder Organisation ihrer Pflicht innert dieser Frist nicht nach, so erlässt das NCSC eine Verfügung über diese Pflicht, setzt darin eine neue Frist und verweist auf die Bussandrohung nach Artikel 74*h*.

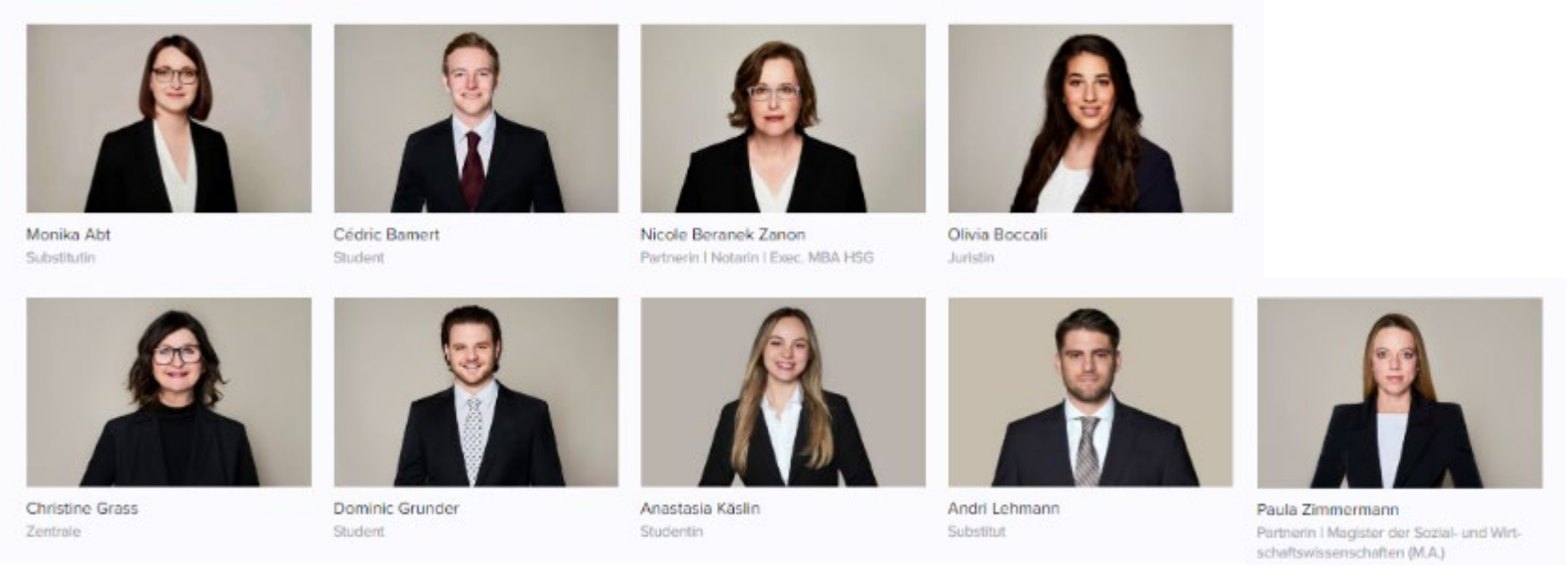
Art. 74h *Missachten von Verfügungen des NCSC*

[1] Mit Busse bis zu 100 000 Franken wird bestraft, wer einer vom NCSC unter Hinweis auf die Strafdrohung dieses Artikels erlassenen rechtskräftigen Verfügung oder dem Entscheid einer Rechtsmittelinstanz vorsätzlich nicht Folge leistet.

[2] Bei Widerhandlungen nach Absatz 1 in Geschäftsbetrieben ist Artikel 6 des Bundesgesetzes vom 22. März 1974[24] über das Verwaltungsstrafrecht (VStrR) anwendbar.

Besten Dank für Ihre Aufmerksamkeit!

Team



HÄRTING

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1

6300 Zug

Switzerland

Tel. +41 41 710 28 50

www. haerting.ch

beranek@haerting.ch