Kellerhals Carrard

Einen Schritt voraus

Praxisrelevantes Rechtswissen zu Cybersecurity und Datenschutz

Dr. iur. Nicolas Mosimann
LL.M., Advokat, Partner
Kellerhals Carrard

Dr. iur. Oliver M. Brupbacher
LL.M., Rechtsanwalt, Partner
Kellerhals Carrard

Seminar Cyber-Gefahren und Datenschutz: Was Schweizer Unternehmen wissen müssen
Arbeitgeberverband Basel
10. Juni 2021

Kellerhals Carrard

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Cybersecurity Risiken im geltenden Recht

Regulatorische Untersuchungen und Sanktionen, insb.

- Mindestanforderungen an die Datensicherheit (*Art. 8 revDSG*)
- Finanzinstitute und Versicherungen (z.B. Art. 14, 23 FinfraG; Art. 3f Abs. 2 BankG)
- Gesundheitswesen (z.B. Art. 12 Abs. 1 lit. b EPDG; Art. 6 Abs. 1, 2 MepV)

Strafuntersuchungen, z.B.

- Verletzung der Datensicherheit (*Art. 61 lit. c revDSG*)
- Geheimnisverletzung (z.B. Art. 35 DSG; *Art. 62 revDSG*; Art. 320 ff. StGB; Art. 47 BankG; Art. 43, 53 FMG; Art. 16 PrHG)

Haftung, z.B.

- der Gesellschaft (z.B. Art. 97 ff.; 41ff. OR; Art. 1, 4 PrHG; Art. 15 Abs. 1 DSG / *Art. 31 Abs. 2 revDSG*; Art. 28 ff. ZGB)
- der Organe (Art. 754, 827 OR)

Ausländische Risiken, z.B.

- *"Companies should avoid generic cyberscurity-related disclosure and provide specific information that is useful to investors."* (SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 21.2.2018)

Dazu kommen u.U.

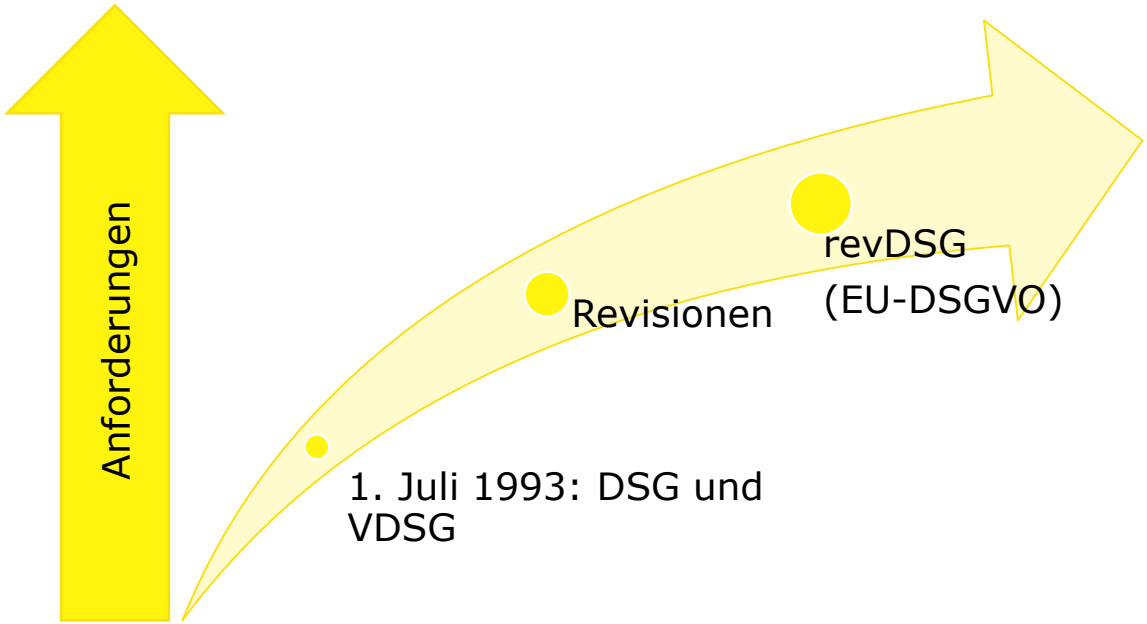
- Datenschäden
- Verlust von geistigem Eigentum, Fabrikations- und Geschäftsgeheimnissen
- Reputationsverlust
- Sach- und Personenschäden
- Betriebsunterbruch

Kellerhals Carrard

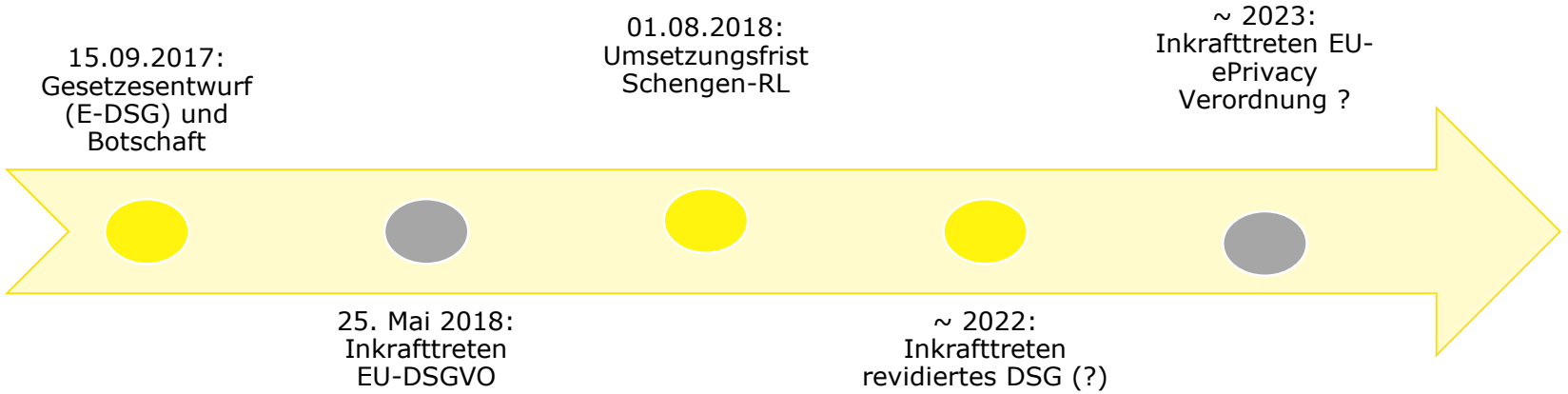
Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Datenschutz in der CH: Eine kurze Geschichte



Fahrplan Schweiz: Im Moment noch Offen



EU-DSGVO: Räumlicher Anwendungsbereich

EU-DSGVO: Geltung in der Schweiz

- Grundsätzlich Anknüpfung am **Ort der Niederlassung**
- **ABER**, auch Geltung wenn:
  - der Verarbeiter gegenüber Personen in der EU **Waren oder Dienstleistungen anbietet** (Sprache, Währung, lokale Domain, Versand an lokale Kunden etc.)
  - der Verarbeiter das **Verhalten** betroffener Personen **beobachtet**, soweit dieses Verhalten in der Union erfolgt (z.B. Tracking, Profiling)

EU-DSGVO: Geltung in der Schweiz

DS-GVO gilt auch für viele Schweizer Unternehmen!

Was sind Personendaten?

Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen	– Kunden- und Mitarbeiterangaben (z.B. Name, Adresse, Geburtsdatum, gekaufte Waren, Notizen zu Meetings, Logs etc.) – Daten juristischer Personen (gemäss *Art. 2 Abs. 1 revDSG* nicht mehr!) – Cookies, IP Adressen?
Besonders schützenswerte Personendaten	– religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten – Gesundheit, Intimsphäre oder Rassenzugehörigkeit – Massnahmen der sozialen Hilfe – administrative oder strafrechtliche Verfolgungen und Sanktionen – *Art. 5 lit. c revDSG: auch genetische und biometrische (identifizierende) Daten, sowie Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen und Daten über Massnahmen der sozialen Hilfe*

Grundsätze der Bearbeitung

Bearbeitung von Personendaten grundsätzlich erlaubt, wenn Grundsätze eingehalten

Bearbeitungsgrundsätze (Art. 4 DSG / *Art. 6 revDSG*)

- Rechtmässig (z.B. berechtigtes Interesse, Einwilligung), nach Treu & Glauben und verhältnismässig
- Zweckgebunden: wie angegeben, aus den Umständen ersichtlich oder gesetzlich vorgesehen (*gemäss Art. 6 Abs. 3 revDSG: "wie vereinbar"*)
- Transparent; für die betroffene Person erkennbar

Sicherstellung der Richtigkeit der Daten (Art. 5 DSG / *Art. 6 Abs. 5 revDSG*)

Sicherheit: Angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten (Art. 7 DSG / *Art. 8 revDSG*)

Ausgewählte weitere Pflichten

Informationspflichten
(*Art. 19 ff. revDSG*)

Auskunftspflichten
(*Art. 25 ff. revDSG*)

Data breach notifications
(*Art. 24 revDSG Meldepflicht an den EDÖB)*

Art. 22 revDSG: Datenschutz-Folgenabschätzung
im Rahmen der Vorbereitung von Projekten

Dokumentationspflicht
als Ersatz der heute geltenden Verpflichtung zur Anmeldung einer Datensammlung beim EDÖB

Melde- und (neu) teilweise Genehmigungspflichten
bei Datentransfer ins Ausland

Zusätzliche Pflichten gemäss EU-DSGVO
- Datenportabilität
- Ernennung eines Datenschutzbeauftragten
- Ernennung eines Vertreters in der EU

Sanktionen

Aktuell

- EDÖB gibt Empfehlungen ab
- Bei Nichtbefolgung oder Ablehnung: Bundesverwaltungsgericht
- Busse von max. CHF 10’000 für vorsätzliche Verletzung bestimmter Pflichten nach DSG

revDSG

- *EDÖB hat Verfügungskompetenz (Erfüllung Anforderung Schengen-RL), jedoch keine Befugnis zu Verwaltungssanktionen (Art. 51 revDSG)*
- *Bussen bis max. CHF 250’000 insb. bei Missachtung von Verfügungen des EDÖB und vorsätzlicher Verletzung bestimmter Pflichten (Art. 63 revDSG)*

EU-DSGVO

- Aufsichtsbehörden mit Kompetenz zur
  - Verfügung von Massnahmen;
  - Verhängung von Bussen bis zu EUR 20’000’000.00 oder 4% des gesamten weltweiten Jahresumsatzes (Bussen auch bei Fahrlässigkeit)
- Verbandsklage im und ohne Auftrag der betroffenen Person

Sanktionen (EU-DSGVO): Erste Bussen*

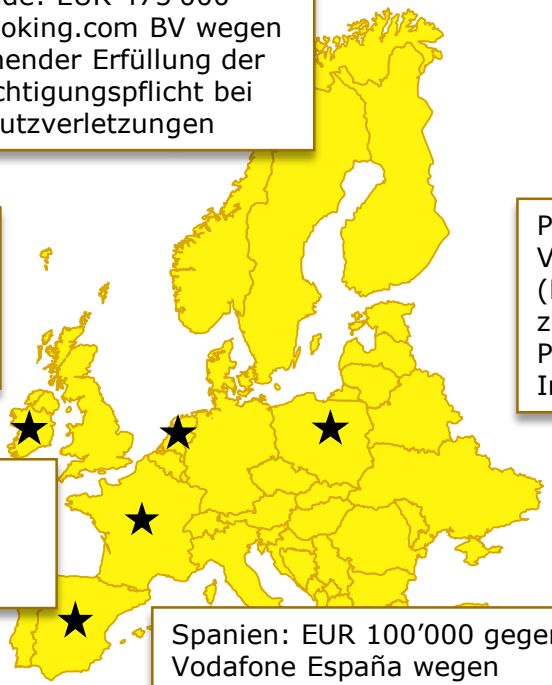
Niederlande: EUR 475’000 gegen Booking.com BV wegen unzureichender Erfüllung der Benachrichtigungspflicht bei Datenschutzverletzungen

Irland: EUR 90’000 gegen CP&A wegen unzureichender technischer und organisatorischer Massnahmen zur Gewährleistung der Informationssicherheit

Polen: EUR 220’000 wegen Verletzun
(Bearbeit
zugänglic
Personen
Informati

Polen: EUR 19’000 wegen unzureichender Erfüllung der

Polen: EUR 18’930 wegen unzureichender Erfüllung der Benachrichtigungspflicht bei Datenschutzverletzungen



Frankreich: EUR 50 M. gegen Google LLC (ungenügende Datenschutz-erklärungen; Anforderungen an Einwilligungen nicht eingehalten)

Spanien: EUR 100’000 gegen Vodafone España wegen unzureichender technischer und organisatorischer Mass-nahmen zur Gewährleistung der Informationssicherheit

* noch nicht rechtskräftig

Personendaten in der Cloud: Beispiel

Die Sorglos Treuhand AG nutzt bis anhin ein auf den eigenen Servern gehostetes CRM. Zukünftig wird sie die SaaS-Lösung der Easy Solution AG nutzen.

Die Easy Solution AG nutzt für Ihre SaaS-Lösung die Cloud von AWS (Amazon). Sämtliche Daten werden somit von der Easy Solution AG resp. AWS im Auftrag der Sorglos Treuhand AG resp. Easy Solution AG bearbeitet/verarbeitet.

Personendaten in der Cloud

Auftragsdatenverarbeitung: Datenverarbeitung durch Dritte als unterstützendes "Werkzeug"

Auftraggeber bleibt verantwortlich

Der Auftragnehmer ist mitverantwortlich

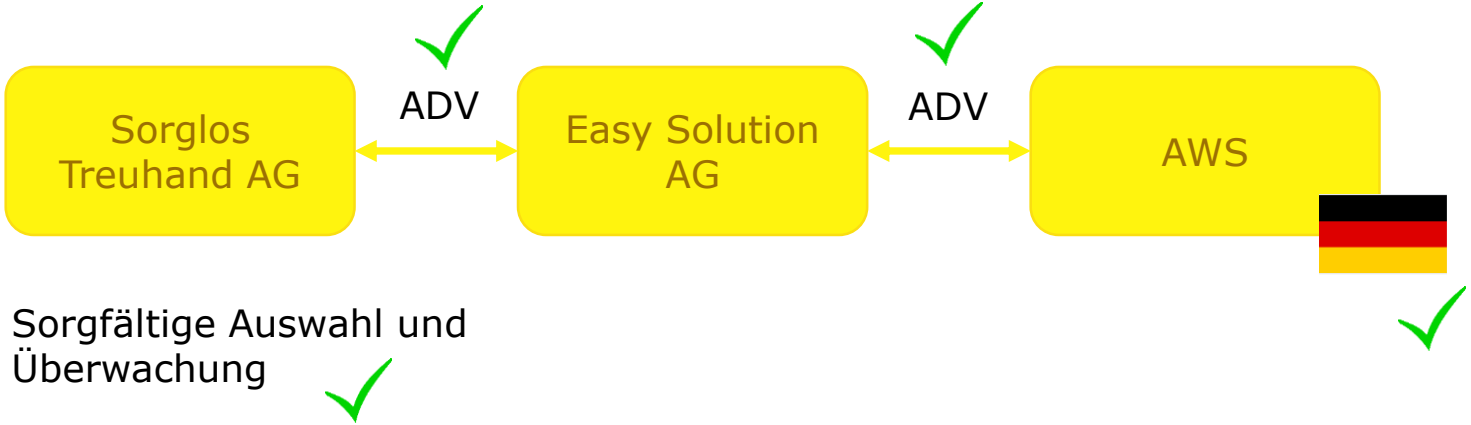
Voraussetzung der Zulässigkeit:

- Sorgfältige Auswahl und Überwachung (hinreichende Garantien, z.B. Zertifizierung?)
- Auftragnehmer ist an Weisungen des Auftraggebers gebunden
- Vertrag in Textform (d.h. auch elektronisch), der detaillierte gesetzliche Vorgaben erfüllt → Standardvertragsklauseln verwenden
- Sub-Auftragsverarbeiter bedürfen Genehmigung

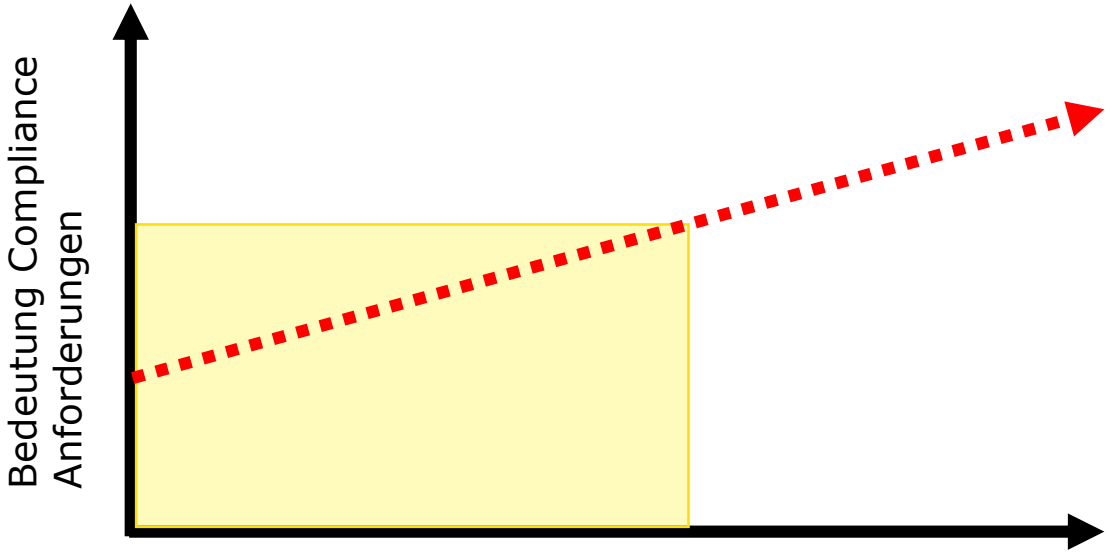
Personendaten in der Cloud: Beispiel

Die Sorglos Treuhand AG nutzt bis anhin ein auf den eigenen Servern gehostetes CRM. Zukünftig wird sie die SaaS-Lösung der Easy Solution AG nutzen.

Die Easy Solution AG nutzt für Ihre SaaS-Lösung die Cloud von AWS (Amazon). Sämtliche Daten werden somit von der Easy Solution AG resp. AWS im Auftrag der Sorglos Treuhand AG resp. Easy Solution AG bearbeitet/verarbeitet.



Bedeutung des Datenschutzes für und Anforderungen an Unternehmen



To Dos

Massnahmen

- Stelle/Abteilung mit Datenschutzkompetenz
- Dokumentation (insb. Verzeichnis von Verarbeitungstätigkeiten)
- Prüfung der Anwendbarkeit von DSG/*revDSG* und EU-DSGVO
- Überprüfung der Rechtmässigkeit der Verarbeitung resp. Einhaltung der Bearbeitungsgrundsätze
- Überarbeitung von Verträgen und Datenschutzerklärungen, insb. Prüfung von Einwilligungen
- Überarbeitung interner Prozesse und Richtlinien (z.B. betreffend Auskunftsrechte, Data Breach Notifications)
- Datenschutzfolgeanalysen
- Abschluss Auftragsdatenvereinbarungen
- Technische und organisatorische Massnahmen

Laissez faire keine Option mehr (Sanktionen!)

Kellerhals Carrard

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Incident: Beginn und Krisenmanagement

From: Peter
To: CEO
Date: Dec 30, 2020 5:30pm CET
Subject: Data Breach Detected

Good Afternoon (and Happy New Year)!

I am an outside consultant, and I have identified what appears to be a serious data breach involving your company's information. This facebook post links to a Google Sheet containing first and last names, social security numbers, email addresses, phone numbers, dates of birth, home addresses, and other identifying information regarding your employees. As you can see, there are over 250k rows of data.

I don't think this should be the type of data that should be publicly available, don't you agree?

As an experienced outside consultant in the cybersecurity field, I am more than happy to help your company in responding to this sensitive situation. Of course, I would expect to be compensated for my time. I have already uncovered more information that I can tell you about once my retainer is paid. My standard retainer is $ 10,000. Additional payment information to follow.

Szenario entwickelt mit Morrison & Foerster LLP (John P. Carlin, David A. Newman und Alex Iftimie)

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Incident: Beginn und Krisenmanagement

Ein Mitarbeiter Ihrer Firma teilt Ihnen mit, dass er auf den Link zu dem facebook-Post geklickt hat und dass Peter Recht hat: Ein facebook-Post von "Streetfighter" enthält einen Link zu einem Google Sheet, das alle Kategorien von Informationen enthält, die Peter beschrieben hat.

Wahrscheinlich hätten auch andere Besucher der facebook-Seite auf den Link klicken und auf dieses Dokument zugreifen können. Der Link wurde kurz vor Weihnachten gepostet.

- **Welche Fragen müssen Sie beantworten, um Entscheidungen zu treffen?**
- **Wer trifft Entscheidungen?**
- **Wer muss an der Reaktion beteiligt werden?**
- **Ist angesichts des Vorfalls eine Benachrichtigung der Mitarbeiter oder der Öffentlichkeit erforderlich?**
- **Müssen Aufsichtsbehörden informiert werden?**

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Incident: Beginn und Krisenmanagement

Meldepflichten im In- und Ausland (Auswahl)

Bei Betroffenheit personenbezogener Daten

- Benachrichtigung der Betroffenen (Art. 4 Abs. 1, 2 DSG / *Art. 6 Abs. 1, 2 revDSG*), insb. falls zum Schutz erforderlich oder vom EDÖB verlangt (*Art. 24 Abs. 4 revDSG*)
- Ausnahmen bei überwiegenden Drittinteressen, wo die Information unmöglich ist / einen unverhältnismässigen Aufwand erfordert (*Art. 24 Abs. 5 lit. a, b revDSG*)
- Benachrichtigung des EDÖB bei einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen (*Art. 24 Abs. 1, 2, 6 revDSG*)
- Keine allg. Pflicht zur Information der Öffentlichkeit (aber Art. 4 Abs. 1, 2 DSG / *Art. 6 Abs. 1, 2 revDSG; Art. 24 Abs. 5 lit. c revDSG*)

Aufsichtsbehörden – branchenspezifische Meldepflichten

- Finanzinstitute und Versicherungen (Art. 29 Abs. 2 FINMAG; FINMA Aufsichtsmitteilung 05/2020; FINMA Rundschreiben 08/25)
- Gesundheitswesen (Art. 12 Abs. 3 EPDV; Art. 66 MepV)

Mi. 30.12.2020 → Mi. 06.01.2021 → Do. 07.01.2021 → Fr. 08.01.2021

Incident: Beginn und Krisenmanagement

Meldepflichten im In- und Ausland (Auswahl)

Offenlegung	– Rückstellungen im Geschäftsbericht (z.B. Art. 960e OR; Art. 49 ff. KR) – Ad hoc-Publizität (Art. 53 KR)
Freiwillige Meldung an Strafverfolgungsbehörden	– Alternativ an Nationales Zentrum für Cybersicherheit (NCSC) oder Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK)
Vertragliche Meldepflichten	– Insb. Auftragsverarbeiter von Personendaten (*Art. 24 Abs. 3 revDSG*) – Insb. gegenüber Versicherern
Ausländische Meldepflichten	- Im Einzelfall abzuklären

Mi. 30.12.2020 → Mi. 06.01.2021 → Do. 07.01.2021 → Fr. 08.01.2021

Incident: Beginn und Krisenmanagement

Die Rolle des Anwalts

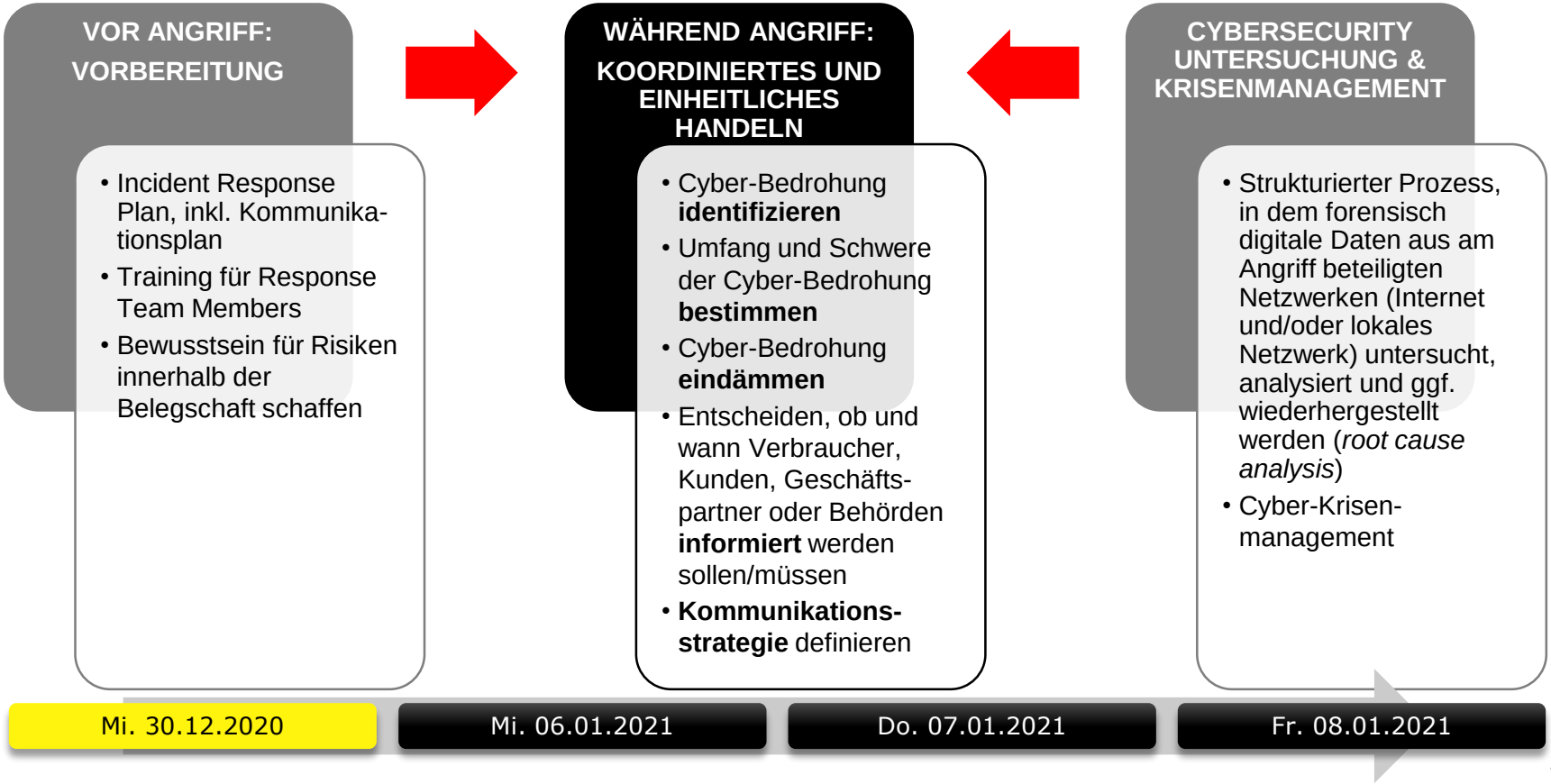
- Identifikation und Analyse rechtlicher Risiken
- Strategische Beratung der Geschäftsleitung
- Governance:
  - Einhaltung des Incident Response Plan des Unternehmens und anderer Prozesse
  - Ordnungsgemässe Dokumentation aller Vorgänge
  - Kommunikationsstrategie und Überprüfung der Statements
  - Einleitung einer vom Anwaltsgeheimnis geschützten internen Untersuchung
  - I.d.R. unter Beauftragung externer Forensiker und IT-Experten
- Beweissicherung / eDiscovery
- Ggf. Einleitung rechtlicher Schritte (Strafanzeige, Zivilklagen, Verteidigung)

Kellerhals Carrard

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Cybersecurity Untersuchungen



Kellerhals Carrard

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Incident: Kommunikation

Telefonkonferenz um 9.00 Uhr CET: Das von Ihnen beauftragte externe Forensikteam hat einen grossen, unbekannten Dateitransfer gefunden, der in den Datenbanken Ihrer Firma ablief und auch Mitarbeiterdaten betrifft, und stoppte ihn. Die Dateien sind verschlüsselt, und ihr Inhalt kann nicht geöffnet werden. Das Team hat keine Hinweise darauf gefunden, dass dieses Problem mit den Mitarbeiterdaten auf facebook zusammenhängt. Die Experten untersuchen gegenwärtig noch, ob der Zugriff und Transfer von Ihrer Firma aus stattgefunden haben könnte.

Anruf um 14:00 Uhr CET: Ein Blogger kündigt an, morgen um 9:00 Uhr CET einen Artikel über eine Datenschutzverletzung betreffend Mitarbeiterdaten bei Ihrer Firma zu veröffentlichen, unabhängig davon, ob Sie einen Kommentar dazu abgeben oder nicht. Ihr CEO möchte der Sache zuvorkommen und eine Pressemitteilung herausgeben. Ihre PR-Firma entwirft ein kurzes Statement:

"We are aware of an intrusion relating to employee information, and our investigation remains ongoing, but at this time, we have no evidence that any information of our customers has been compromised."

- **Wie ist Ihre Reaktion auf das Statement?**
- **Wie reagieren Sie auf die Anfrage des Bloggers?**

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Incident: Kommunikation

- Herausforderungen an die Kommunikation bei Cyber Incidents sind erheblich
  - Daher: Frühzeitig Experten einschalten und Prozesse etablieren
- Ausgangspunkt der Kommunikationsstrategie: Rechtliche Strategie
- Zur Vorbereitung auf Cyber Incidents gehört ein schlüssiges und widerspruchsfreies Standby Statement (SBS) und ein Q&A

- Verhalten, das die Reputationsrisiken erhöht und zu vermeiden ist:
  - Aussagen als gesichert erscheinen lassen, die tatsächlich ungesichert sind
  - Widersprüche zwischen SBS und Handeln des Unternehmens
  - "PR-Reinwaschung" und "scheibchenweise Information
  - Inkonsistente Kommunikation (bei Pressemitteilungen, Behörden, FAQs, öffentliche Erklärungen, Call-Center-Antworten auf Kundenanfragen etc.)

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Kellerhals Carrard

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Ransomware

From: CISO
To: CEO
Date: Jan 7, 2021 6:30pm CET
Subject: Cyber threat

Bad news. The forensics team has now found artifacts of exfiltration of client data – and indications that the same intruder is elsewhere on the broader company network.

We now think that the bad actor's point of entry into our systems wasn't through a vulnerability of our systems, but through our own staff clicking the link to the facebook post in Peter's first email. So Peter appears connected to the bad actor (or possibly is the bad actor).

In certain emails, the link was doctored to be identical to the actual facebook post link but contained hidden scripts that launched when clicked. We don't know how it got past our phishing filters.

- **Was sollten Sie jetzt tun?**
- **Sollten Sie die Strafverfolgungsbehörden einschalten?**
- **Was sind die Risiken und der Nutzen des jeweiligen Vorgehens?**

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Ransomware

From: Peter
To: CEO
Date: Jan 8, 2021 11:30pm CET
Subject: Re: Data Breach Detected

Uh oh, looks like you found me! It's unfortunate that you terminated the exe I was running, but no worries- there's plenty more where that came from :-) I already have over 1TB of data from you! If only you managed to find my exe and terminate it sooner... I even gave you a hint earlier!

I guess I can tell you now about the other information I alluded to in my first email. Your client relationships are really interesting. I'm sure the world would like to know more about them! Of course, you might be able to convince me otherwise by paying my retainer fee... And I would much prefer to deal with you privately instead of all those fake news outlets.

Also, I did leave something behind that I thought you would appreciate...

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Ransomware

This machine has been encrypted with the strongest encryption. The ONLY decryption key is stored on a secret Internet server. Nobody can decrypt your files until you pay and obtain the decryption key. Time is money. You have 48 hours to submit payment of $25,000 in Bitcoin. If you do not send money in that time, your files will be permanently encrypted and the decryption key will be destroyed.

Click on this link to connect to the secret server and follow instructions.

Mi. 30.12.2020 | Mi. 06.01.2021 | Do. 07.01.2021 | Fr. 08.01.2021

Ransomware

Bezahlen oder nicht bezahlen?

- "*Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations.*"
  (OFAC Advisory on Potential Sanctions Risks for Facilitating Ransomware Payment, 1.10.2020)
- Risiken:
  - Verletzung von Wirtschaftssanktionen
  - Materielle Unterstützung des Terrorismus
  - Reputationsrisiken
  - Wiederholungsrisiken

Cyber Risk Versicherung

- Breite Verfügbarkeit
- Grundvoraussetzung i.d.R. Implementierung eines Cyber Risk Managements
- Deckungsbedingungen teilw. umstritten, z.B. war exclusion (*Mondelez Int., Inc. v. Zurich American Insurance Co.*, No. 2018L011008, 2018 WL 4941760, Ill. Cir. Ct., Oct. 10, 2018), sanction limitation

Kellerhals Carrard

Agenda

1. Cybersecurity Risiken im geltenden Recht
2. Datenschutz "in a nutshell"
3. Incident: Beginn und Krisenmanagement
4. Cybersecurity Untersuchungen
5. Incident: Kommunikation
6. Ransomware
7. Lessons Learned

Lessons Learned

– Datenschutz-Compliance

– Expertise und Koordination des internen und externen Response Teams

– Schnelligkeit und Entscheidungsbefugnis

– Strategischer Ansatz

– Vorbereitung (IR-Plan, Kommunikationsplan)

– Einübung des IR-Plans

– Business Continuity Plan (z.B. Back-up Systeme)

– Reibungsloser Informationsfluss im Unternehmen

Kellerhals Carrard

Ihr Kontakt: Dr. Nicolas Mosimann, Dr. Oliver M. Brupbacher

Kellerhals Carrard Basel KlG
Henric Petri-Strasse 35
P.O. Box 257
CH-4010 Basel

+41 58 200 30 00

nicolas.mosimann@kellerhals-carrard.ch
oliver.brupbacher@kellerhals-carrard.ch