LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Cyber Security Incidents – How to avoid legal risks in Germany and Switzerland?

Thursday, 17 June 2021 | 4:30 – 6:00 p.m. (CEST)

Agenda

I. Introduction

- Examples of cyber attack cases
- General introduction to Cyber Security Incidents

II. Cyber Security Incidents: Risks & Strategies

- Overview of the legal framework and respective challenges
- Risks and management of Cyber Security Incidents
- Management liability for Cyber Security Incidents

III. Consequences of Cyber Security Incidents: Defending against Fines and Claims

- Overview of imposed fines: national and international
- Current developments in courts rulings and case studies
- Basics regarding GDPR claims and GDPR claims as a business model

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Introduction

Wave of Ransomware Attacks in Switzerland

- Data on the computer is no longer available or is encrypted
- Damage control
- Identification of infected systems
- Detection
- Criminal complaint
- Payment of ransom?
- Forensic investigations?
- Backup of encrypted data
- Reinstallation of the affected systems

Source: www.entec.ch and https://www.ncsc.admin.ch

Possible Explanations for Ransomware Attacks

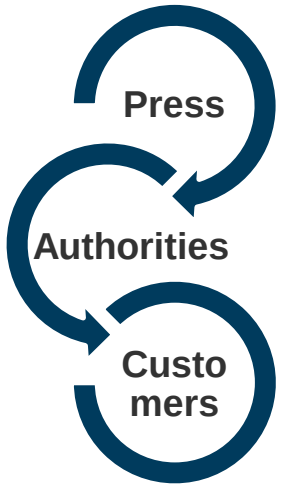
- Change of focus of cyber criminals from B2C to B2B (=deep pockets)
- Switzerland popular location for data centers
- Switzerland has many EMEA headquarters
- Swiss companies massively underestimate how to deal with cyber attacks and are not prepared
- «Employee Awareness» is insufficient - attacks are 99% spear phishing emails that employees open by mistake
- No interest in implementing IT standards (e.g. ISO)
- Lack of law enforcement

Cyber Security Incidents – Case Study

- **Case Study**
  A bank promises its customers various non-cash prizes as part of a prize draw. In order to participate in the sweepstakes, customers must register online and provide their personal data.

- **Data Breach**
  Following a data breach, address details, account numbers, telephone numbers and e-mail addresses of **20,000 customers**, who have registered for the lottery, appear freely accessible on the Internet

- **Consequences**



- Data breach becomes public
- The data protection authorities conduct investigations
- Customers start to claim damages

Cyber Security Incidents – Legal Framework (EU)

- **Art. 32 GDPR: Data Security**
  Controllers (Art. 4 (7) GDPR) and Processors (Art. 4 (8) GDPR) are required to implement suitable technical and organizational measures in order to ensure an appropriate level of data security

- **Art. 4 (12) GDPR: Personal Data Breach**
  "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*"

- **Art. 5 para. 1 lit. f GDPR: Integrity and Confidentiality**
  Personal data needs to be… *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*"

Cyber Security Incidents - Legal Framework (CH)

- **Art. 8 para. 1 and 2 rev. FDPA**
  (1) The controller (Art. 5 lit. j rev. FDPA) and the processor (Art. 5 lit. k rev. FDPA) shall ensure data security appropriate to the risk by taking suitable technical and organizational measures. (2) The measures must make it possible to avoid breaches of data security.

- **Art. 5 lit. h rev. FDPA: „ Data security breach“**
  "A breach of security that results in personal data being inadvertently or unlawfully lost, deleted, destroyed, or altered, or disclosed or accessed by unauthorized persons".

Consequences & Risks (EU)

- **Notification Obligations**
  - **Art. 33 GDPR**: Obligation of the controller to notify the competent authority - within 72 hours
    - Obligation mainly depends on the relevant risks involved, recital 85 s. 1 GDPR
  - **Art. 34 GDPR**: Obligation of the controller to notify the data subject in the event of a high risk to personal rights and freedoms - without undue delay

- **Risks regarding Fines**
  - Fines for breach of notification obligations under Art. 33, 34 GDPR
  - Fines due to insufficient data security
  - Fines due to violations when involving data processors
  - Fines due to violations of other requirements of the GDPR

- **Reputational risks as well as risks for existing business relationships**

- **Mass claims for damages by data subjects**

Consequences & Risks of Data Breaches (CH)

- **Reporting requirements**
  - Art. 24 para. 1 rev. FDPA: Obligation of the person responsible to notify the competent authority - as soon as possible
  - Art. 24 para. 3 rev. FDPA: Obligation of the processor to notify the controller - as soon as possible
  - Art. 24 para. 4 rev. FDPA: Obligation of the controller to notify the data subject if it is necessary for his or her protection or if the competent authority so requires

- **Risks relating to fines**
  - Fine up to CHF 250'000 – ad personam (!)
  - No fines for violation of reporting obligations under Art. 24 rev. FDPA
  - Fines for insufficient data security: Art. 61 let. c rev. FDPA
  - Fines due to errors in the engagement of processors: Art. 61 let. b rev. FDPA
  - Fines for violations of other provisions of the revised FDPA

- **Reputational risks and risks to existing business relationships**
- **Lawsuits / claims for damages from affected persons rather rare**

Liability of Management (DE)

- **Directors' and Officers' Liability:**
  In Germany particularly regulated in:
  - **Sec. 93 Stock Corporation Act** (*AktG*): members of the management boards‘ liability
  - **Sec. 43 Limited Liability Companies Act** (*GmbHG*): directors‘ liability

- **Main prerequisite for damage claims:**
  Breach of duty - standard: care of a prudent manager faithfully complying with his duties

- **Supervisory board‘s supervisory duty**

- **Inadequate IT security as a violation?**
  Some authors confirm this view, resulting in the company being allowed to assert damages from the board member or managing director

- **Practical relevance to date**

Liability of Management (CH)

- **The member of the Management Board shall be liable if the following conditions are met:**
  - Position and activity as a member of the Management Board
  - Breach of duty
  - Negligent or intentional conduct
  - Damages
  - No exculpation and causality
  - Right to assert liability claims
  - Burden of proof

- **Who can sue**
  - Shareholder
  - Creditors
  - Company

Preparatory Measures

- **Resources**
  Companies must have an effective data protection organization in place that is adequately funded and staffed

- **Essential:**
  - Company-specific risk analysis
  - Careful selection, instruction and monitoring of employees
  - Organization of operational data protection in accordance with the requirements of Art. 24 (1) and 5 (2) GDPR and actual enforcement of these requirements in practice

- **Documentation**
  Comprehensive and legally compliant documentation of respective structures and processes

- **IT Security**
  Documentation of contracts concluded with IT service providers (in advance) and agree on technical and organizational measures to ensure an appropriate level of data security

Strategy for the Defense against Cyber Security Incidents

- Regular installation of security updates of the operating system as well as installed programs
- Updating the antivirus program used
- Installation of a firewall
- Critical handling of personal data
- Use of secure passwords (at least 8 characters, consisting of numbers, upper and lower case letters and special characters such as «@»; regular renewal)
- Create backups (backup copies that restore data or photos, for example, in the event of data loss)
- Checking the security status of the computer

Cyber Security Incident Response Plan

- **Cyber Security Incident Response Plan (CIRP)**
  Preparation of a CIRP is critical to mitigate the risk of damage claims

- **Assignment of tasks and measures**
  Project planning, project management and appointment of a task force: executives, IT security, risk management, data protection officer, legal department, communications department and others

- **Fact finding**

- **Communication**
  Information of employees, legal information and co-determination rights of the works council, communication with authorities

- **Documentation of the incident and the measures taken**
  Causes of the incident, measures taken to clarify the facts, circumstantial evidence obtained, steps taken to limit damage

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Defending against GDPR Fines

Please vote now

What was the highest GDPR fine imposed by a German supervisory authority to date?

GDPR Fines – Overview (Germany)

EUR 0,3 mio.	▪ Soccer club in southern Germany (LfDI Baden-Württemberg, 10 March 2021) ▪ Negligent violation of the duty of accountability within the meaning of Art. 5 (2) GDPR
EUR 10,4 mio. not yet final, the company has lodged an appeal	▪ Hardware-Supplier (LfD Niedersachsen, 8 January 2021) ▪ Illegitimate video surveillance of employees and customers over a period of at least two years
EUR 35,2 mio.	▪ Fashion company (HmbBfDI, 1 October 2020) ▪ In the opinion of the authority, implementation of disproportionate control measures that affected hundreds of employees of the Nuremberg Service Center
EUR 1,2 mio.	▪ Health insurance company (LfDI Baden-Württemberg, 30 June 2020) ▪ Use of data of around 500 people who previously participated in a giveaway for marketing purposes
EUR 9,5 mio. / EUR 0,9 mio.	▪ Telecommunication company (BfDI, 9 December 2019) ▪ Unauthorized persons were able to obtain customer data due to insufficient authorization in the customer service process
EUR 14,5 mio. / not yet final	▪ Real estate company (BlnBDI, 5 November 2019) ▪ Data storage of former tenants in an archive without a legal basis and without a possibility for deletion

FDPA and GDPR Fines (CH) I

- **Under the current FDPA maximum fines "only" CHF 10'000**
  Virtually no fines and case law. Practically no statistics

- **Revised FDPA introduces fines up to a maximum of CHF 250'000**
  Fines will be imposed for the following violations:
  - in the case of intentionally false, incomplete or omitted information about data processing (Art. 60 para. 1 rev. FDPA)
  - in the event of insufficient cooperation with the FDPIC (Art. 60 para. 2 rev. FDPA)
  - in the event of a breach of the duty to inform about automated individual decisions (Art. 60 para. 1 let. a rev. FDPA)
  - in the event of non-compliance with an order of the FDPIC (Art. 63 rev. FDPA)
  - in the event of a breach of data security and export restrictions (Art. 61 let. a and c rev. FDPA)
  - in the event of defective appointment of the order processor (Art. 61 Bst. b rev. FDPA)
  - in case of breach of professional secrecy (Art. 62 rev. FDPA)

FDPA and GDPR Fines (CH) II

- **Ad Personam (!)**
  - According to the white paper and statements in the legislative process, fines are targeted at management personnel. However, it cannot be ruled out that fines will be imposed on executive employees without a management function.
  - Fines will only be imposed on the company if the effort to identify the offending person is disproportionate. In such a case, the maximum fine is CHF 50,000.
  - But: only in case of intent or contingent intent

- **Notification requirement in Switzerland?**
  - Under the current FDPA, no notification obligation for cyber security incidents.
  - However, there are sector-specific notification obligations (e.g., in the financial and energy sector)

- **GDPR directly applicable - but no direct enforcement of fines possible in Switzerland yet. Federal Council can conclude state treaties**

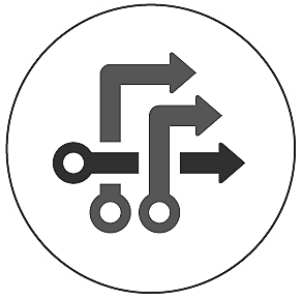
- **Depending on the constellation, not all GDPR provisions directly applicable to Swiss companies: e.g. Art. 56 (lead supervisory authority)**

GDPR Fines – Overview (EU)

EUR 28 mio.	▪ Telecommunication company (Garante) – Italy, 15 January 2021) ▪ Several million marketing calls without consent, information deficits in Apps and insufficient technical-organizational measures
EUR 60 mio. & EUR 40 mio.	▪ Leading technology company (CNIL – France, 7 December 2020) ▪ Use of tracking-cookies for marketing purposes without consent of the data subject and missing privacy policies
EUR 20 mio.	▪ Hotel company (ICO – UK, 30 October 2020) ▪ Unknown hackers were able to obtain personal data of 339 million hotel guests over multiple years
EUR 450 k.	▪ Communications platform (Data Protection Commission – Ireland, 9 December 2020) ▪ Violation of notification obligations after data breach
EUR 475 k.	▪ Travel marketplace (Autoriteit Persoonsgegevens – Netherlands, 10 December 2020) ▪ Violation of notification obligations after data breach

Legal Framework

Sec. 130, 30 of the Act on Regulatory Offences (OWiG) establish the legal basis for imposing fines on companies in Germany



Direct Liability?

Under OWiG, companies cannot be held liable directly

Attribution

A fine may only be imposed on a company if a „*linked offence*“ (*Anknüpfungstat)* has been committed

Linked offence

A violation committed by someone in a management position, e.g. a violation of a duty of supervision

Exception under GDPR?

It is highly disputed if these principles also apply with regard to GDPR fines

Please vote now

Do the German data protection authorities take the view that companies can only be held liable for data protection violations if an employee in a management position violated his/her duties?

Legal Framework in Germany

The German Data Protection conference adopted a resolution on 3 April 2019 stating that Sec. 130, 30 OWiG do not apply in terms of GDPR violations.

Sec. 130, 30 OWiG

These norms do not apply to GDPR violations

“Management Position“

Companies can be held liable regardless if the violation has been committed by someone in a management position

Employees

Companies can be held liable for GDPR violations committed by their employees

Recent Court Rulings: DC Bonn (11 Nov 2020)

The Case

A person who called a company's call center managed to gain knowledge of a customers phone number.

The caller provided the name and the date of birth of said customer.

Authorities' action

The data protection authority imposed a EUR 9.55 million fine on the telecommunications company.

The authority argued that the company had failed to implement appropriate technical and organizational measures to comply with Art. 32 GDPR (security of processing)

The Court's ruling

The court ruled that companies can be held liable directly under the GDPR. Sec. 130, 30 OWiG do not apply.

The court reduced the fine to EUR 900 k.

Recent Court Rulings: DC Berlin (18 Feb 2021)

The Case & authorities' action

The Berlin DPA fined a company for allegedly not implementing the necessary technical and organizational measures to comply with GDPR data deletion requirements.

The authority imposed the fine directly on the company.

The Court's ruling

The court ruled that the fine-notice is invalid. Companies can not be held liable directly under the GDPR.

Sec. 130, 30 OWiG apply; it is therefore necessary that the authority proves a violation committed by an employee in a management position.

Status quo

The public prosecutor’s office has filed an immediate appeal.

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Defending against GDPR Claims

Please vote now

What was the highest amount of damages awarded by a German court to date due to a GDPR infringement?

Recent court rulings awarding damages (excerpt)

EUR 800 LC Hildesheim, 5 October 2020	The concept of non-material damage is to be interpreted broadly (deterrent effect)
EUR 300 Higher Labour Court Cologne, 14 September 2020	Claims for damages under the GDPR should have an educational effect
EUR 1.500 Labour Court Dresden, 26 August 2020	Claims for damages should have a deterrent effect
EUR 1.500 Labour Court Neumünster, 11 August 2020	Claims for damages should have a deterrent effect
EUR 1.000 DC Darmstadt, 26 May 2020	The loss of control over data causes damage
EUR 5.000 Labour Court Düsseldorf, 5 March 2020	The effective sanctioning of GDPR violations can only be achieved through a deterrent effect of claims for damages

Recent court rulings denying damages (exerpt)

CoA Stuttgart 31 March 2021	No shifting of the burden of proof or facilitation of evidence – the rules of evidence of the Code of Civil Procedure (*ZPO*) do apply
DC Frankfurt a. M. 18 January 2021	The plaintiff must demonstrate that damage has occurred
CoA Dresden 12 January 2021	Claims for damages require either a serious interference with personality or some other significant impairment
CoA München 8 December 2020	A less serious violation of the right of personality may, under certain circumstances, constitute non-material damage (blocking of a user profile not sufficient)
DC Landshut 6 November 2020	Damages for pain and suffering under the GDPR are not to be awarded for a minor breach without serious prejudice

Learn more

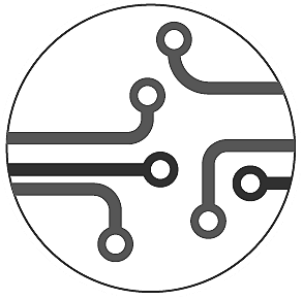
https://www.lw.com/thoughtLeadership/GDPR-Violations-in-Germany-Civil-Damages-Actions-on-the-Rise

Conditions for Liability, Art. 82 GDPR

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

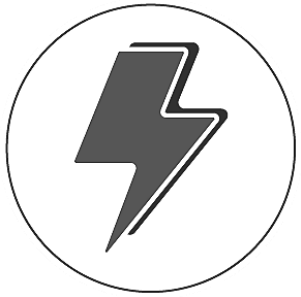
Addressee

Art. 82 GDPR addresses the controller or the processor



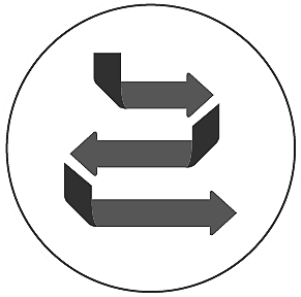
Infringement

Most likely based on insufficient data security or violations regarding the right of access



Damage

Material or immaterial (non-material) impairments



Causality

The damages must be a result of the infringement

Damages within the meaning of Art. 82 GDPR

Damages can be of material or immaterial nature. The extent of the concept of damages is highly disputed in case law.

Extensive Approach

A slight impairment can lead to claimable damages

Restrictive Approach

The GDPR violation must lead to a concrete, not merely insignificant or perceived violation of personal rights

Risk of abuse

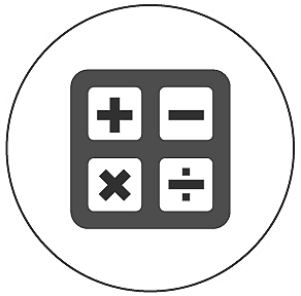
A trivial impairment does not justify immaterial damages

Litigation financiers

Publicized fine proceedings or data breaches increasingly call commercial litigation financiers or specialized consumer attorneys to the scene.

Advertisements

Specific marketing to obtain assignments of claims



A known business model

Business model of litigation are already established in other areas of law - such as compensation claims against airlines

Examples

Kleinfee, EuGD, RightNow

Defense against Claims for Damages (CH)

- **In general: actions for damages in Switzerland rather rare**
- **Art. 82 GDPR: no analogous provision in Switzerland**
- **Art. 32 rev. FDPA refers to actions for the protection of personality are governed by Articles 28, 28a and 28 g-28l of the Civil Code:**
  - Existence of an unlawful violation of personality rights
  - Damages, claim for restitution of profits, compensation, injunctive relief, etc.
- **Costs and cost risk for affected persons usually too high**
- **Proof of damage very difficult to provide**
- **The civil law instrument of "mass actions" is not known as such in Swiss data protection law**
- **Therefore FDPA damages claims not (yet) a business model in Switzerland**

CoA Stuttgart (31 March 2021)

The Case

A credit card company was subject to a cyber attack. The hackers illegitimately accessed customers' personal data and published it online.

A plaintiff sued for damages, arguing that the principle of data security and the right to access (Art. 15 GDPR) have been violated.

The courts' ruling

The court did not award damages, arguing there has neither been a GDPR violation nor causality.

In addition the court decided that the GDPR does generally not warrant a shifting of the burden of proof or facilitation of evidence (exceptions apply).

Status quo

The decision is not yet final. An appeal has been lodged.

Involvement of CJEU

On April 15, 2021, the Austrian Supreme Court referred the following key questions regarding non-material damages for data protection violations under Art. 82 GDPR to the CJEU. The Decision is likely to have significant implications for ongoing and future proceedings.

1. **Breach equals infringement (?)**
   Is the breach of provisions of the GDPR as such sufficient for the award of damages?

2. **EU law requirements**
   In addition to the principles of effectiveness and equivalence, does EU law impose further requirements that national courts must observe when assessing damages under Art. 82 GDPR?

3. **Materiality threshold**
   Does non-material damage require a consequence (or consequence of the infringement of at least some weight) that goes beyond the annoyance caused by the infringement?

LATHAM & WATKINS LLP

NIEDERER KRAFT FREY

Your Questions

Clara-Ann Gordon

Technology (M&A & Litigation), *Data Privacy, Dispute Resolution, Partner, DPO,*
Zurich

T +41.58.800.8426
E clara-ann.gordon@nkf.ch

Tim Wybitul

Data Privacy (Litigation & Trial),
Partner, DPO,
Frankfurt am Main

T +49.69.6062.6550
E tim.wybitul@lw.com

Disclaimer

This presentation is prepared as a courtesy to Latham clients and friends of the firm. It is not intended to, and shall not, create an attorney-client relationship between any viewer and Latham & Watkins LLP, nor should it be regarded as a substitute for consulting qualified counsel. If you require legal advice concerning this or any other subject matter, do not rely on this presentation, but rather please contact your Latham & Watkins LLP relationship attorney, who can assist you in securing legal advice tailored to your specific situation.

The presentation is not created or designed to address the unique facts or circumstances that may arise in any specific instance, and you should not and are not authorized to rely on this content as a source of legal advice and this seminar material does not create any attorney-client relationship between you and Latham & Watkins.