International Distribution Institute

Panel Discussion

Sanctions for non-compliance with the protection of personal data

Mariaelena Giorcelli
Michael K. Lindsey
Alexandra Mendoza-Caminade
Carlo Piltz
Felipe Toscano

The legal framework under GDPR

- In order to assure an efficient protection of personal data it is necessary to have **equivalent sanctions in all Member States** (§ 11, 13, 129 of the Whereas)

- sanctions have to be **effective**, **proportional** and **dissuasive**

- Sanctions: administrative fines / penalties

Administrative fines under GDPR

Elements to be considered while issuing an administrative fine (Article 83):

a) nature, gravity and duration of the infringement

b) intentional or negligent character of the infringement

c) action taken by the controller or processor to mitigate the damage

d) degree of responsibility of the controller or processor

Administrative fines under GDPR

e) previous infringements

f) degree of cooperation with SA

g) categories of personal data affected

h) manner in which the infringement became known

i) previous orders of SA

j) adherence to approved codes of conduct /certification

k) other aggravating or mitigating factor applicable to the circumstances of the case

Administrative fines under GDPR

Amount of the administrative fines:

up to **10 000 000 EUR**, or in the case of an undertaking, up to **2 %** of the total worldwide annual turnover of the preceding financial year, whichever is higher

For stricter infringements

up to **20 000 000 EUR**, or in the case of an undertaking, up to **4 %** of the total worldwide annual turnover of the preceding financial year, whichever is higher

The French legal framework

- A very complex normative set

- Law relating to data, files and freedoms: January, 6th 1978
- Law for a Digital Republic: October 7th, 2016

- GDPR 2016/679 of April 27, 2016

- Law on the Protection of Personal Data : June 20, 2018 - Decree of August 1st, 2018

- "Ordonnance": December 12th, 2018 **amending the 1978 Law (rewriting the Law)**

- A mission of control facilitated for the CNIL

- Broader definition of the places to be controlled

- Limitation of professional secret
- Online check possible under a false identity by agents of the CNIL

- An enhanced sanctioning power: « corrective powers » against controllers or processors

- a warning
- a notice
- a financial penalty
- a measure specific to an emergency situation in case of violation of rights and freedoms.

- The expansion of the group action

- GDPR flexibility used by France
- Before: only for the cessation of the breach
- Today: also the reparation of the prejudices.

The German legal framework

The German implementation

- In account of the German federalism:
  - one DPA per federal state (= 16),
  - Bavaria has two: one for the private and one for the public sector entities and
  - one federal DPA, mainly for the federal agencies.
  - All in all: 18 DPAs with different interpretations of GDPR.
- No fines against public authorities (sec. 43 (3) German Federal Data Protection Act (BDSG)).

The Brazilian legal framework

Brazilian Data Protection Law: enacted on August 2018, with a 2-year *vacatio legis*

- Data leak cases currently analyzed according to general principles of Civil and Criminal Law, as well as the Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet* – Law no. 12,965/14)

- Legal framework very similar to the European GDPR (extraterritorial applicability, clear consent, right to access, privacy by design, among others)

Brazilian Data Protection Authority: created to analyze and render decisions regarding data leak cases and enact new rules pertaining to the subject

- Authority also crated to ensure surveillance, regulation, promotion of best practices, administrative and other related support (similar to local antitrust and stock exchange authorities, among others)

- An agency of the President's Office, and the 5 members of its Board of Directors are nominated by the President

Sanctions under the new Brazilian Data Protection Law:

(i) warning, with a deadline for implementing the necessary measures to remedy the violation;

(ii) monetary fine, of up to 2% of the legal entity or economic group's revenue in the preceding fiscal year, excluding taxes paid, limited to R$ 50 million per violation;

(iii) daily monetary fine, limited to the total amount of R$ 50 million per violation;

(iv) public disclose of the violation, once it is duly assessed and confirmed;

(v) blocking of the personal data related to the violation until its remedied; and/or

(vi) elimination of the personal data related to the violation in question.

United States

Federal Enforcement

- No centralized, comprehensive national information security law
- Unlike GDPR, U.S. takes a sectoral approach:
  - Securities: Sarbanes-Oxley Act
  - Financial:
    - Gramm-Leach-Bliley Act Safeguards Rule
    - Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
      - Office of Comptroller of the Currency, Federal Reserve Board and Federal Deposit Insurance Corporation
  - Health:
    - Health Insurance Portability and Accountability Act Security Rule
    - Health Information Technology for Economic and Clinical Health Act
  - Homeland Security Act including Federal Information Security Management Act

U.S. Federal Trade Commission

- Primary federal authority for enforcement of privacy and data security requirements
- Enforcement authority: FTC Act § 5
  - "**unfair**" prong
  - "**deceptive**" prong
- Potential for officers' personal liability -- *FTC v Commerce Planet, Inc.* (9th Cir 2016)($18.2 million)

State Enforcement: California

California Consumer Privacy Act

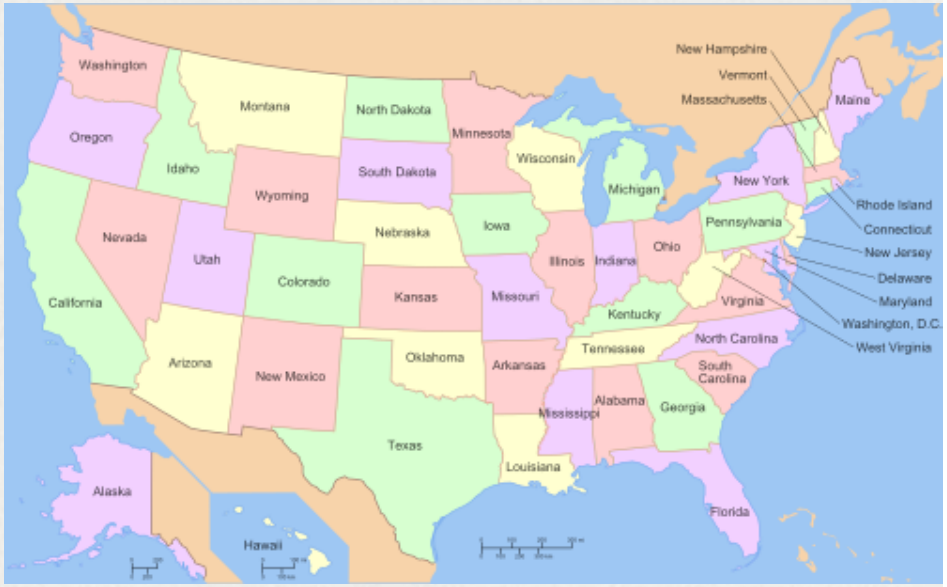
- Goes into effect 1 January 2020
  - Amendments to law still being proposed / considered
  - Regulations still being developed; expected in October
- Applicable to for-profit businesses that
  - Collect and control CA residents' PI;
  - Do business in CA (broadly defined); and
    - Have annual gross revenues greater than $25M;
    - Receive or disclose PI of 50,000 CA residents, households or devices; or
    - Derive 50% of annual revenues from selling CA residents' PI
- Potential penalties for non-compliance
  - Attorney General: $2,500 - $7,500 per violation
  - Private action damages: between $100 and $750 per incident OR actual damages, whichever is greater
  - Injunctive or declaratory relief
  - Any other relief court may deem proper

State Enforcement: California

Individual Rights	GDPR	CCPA
Right to be informed	X	X
Right to object	X	X
Right of access	X	X
Right to rectification	X	
Right to erasure / consent withdrawal	X	X
Right to restrict data processing	X	
Right to transparency		X
Right to data portability	X	
Right to object to automated processing and profiling	X	
Right to non-discrimination for exercising privacy rights		X

State Attorneys General

- Many states have “little FTC Acts”
- State attorneys general have obtained large “resolution payments” in privacy and data security cases
- Often the first notified of a potential privacy or security issue
- State data security breach notification laws
  - All 50 states, D.C., Guam, Puerto Rico and the Virgin Islands
  - Basis for tens of millions of breach notification letters sent



Payment Card Industry Security Standards Council

- Made applicable to merchants via agreements with brands or merchant banks
- Potential for issuance of large fines
- Limited ability to appeal
- Cited by some state AGs in enforcement actions

Case study - Brazil

NETSHOES (one of the biggest sports and shoes ecommerce in Brazil)

- First denied the data leak (of course people uncovered the truth)
- Only recognized the mistake after a notice was sent to the USA Securities and Exchange Commission
- Leaked data: name, date of birth, ID number, purchase history and shopping preference of almost 2 million clients (no credit cards, passwords or other sensitive financial information involved)
- Leaked data from clients that work in government agencies (President's Office, Supreme Court, Federal Police, House of Representatives, among others)
- Sanction: payment of a R$ 500,000 fine to a public fund for repair of collective damages and commitment to improve its cyber protection system, subject to being sued by the Public Attorneys for up to R$ 95 million in case of non-compliance or a new data leak

Case study - Brazil

BANCO INTER (bank that operates 100% digitally)

- At first, in addition to denying the fact, they hired bots to comment on news, articles and social media posts that these were fake news (later called the ‘bank fanbots’)
- According to the Public Attorney’s accusation, the bank also threatened a researcher that was studying the case and posting updates on the internet
- Leaked data: personal information, photographs of checks, documents, credit cards of clients, passwords and related data of almost 100.000 people (including employees, officers and board members of the bank)
- Sanction: payment of a R$ 1,5 million fine to charity and public institutions that fight cyber crimes

Recommended actions:

Before a data leak occurs:

- Hire a data leak insurance (or a general cyber-crime insurance)
- Structure the data protection guidelines, services providers and related departments of the company according to the new law
- Review and update the privacy policies and terms of use of websites and related documentation according to the new law
- Hire a company to assess and/or monitor the risks of data leak

Recommended actions:

After a data leak occurs:

- Hire a PR exclusively to handle the case
- Never deny the fact to preserve the company's image (it will be worse if the leak actually happened and people figure out that the company is trying to hide the truth)
- Assemble a team to focus in calling all clients and people whose data was leaked to show that the company cares and is acting proactively to contain such leak
- Support the Public Attorney's investigation

Insurance

- Brazilian insurances market is strongly regulated
- Data leak insurance was only officially approved by the Brazilian authority on November 2018
- Mostly international insurance companies offering such kind of insurance in Brazil due to high costs and no expertise of local companies
- No case law yet
- One big local insurance company involved in a recent data leak scandal, but no official investigation or formal process has been initiated yet

Which sanctions in France?

Sanctions by the CNIL in 2018

- 49 formal notices
- 11 sanctions were pronounced by the restricted formation:
  - 10 pecuniary sanctions (including 9 public and 7 concerning breaches of the security of personal data)
  - 1 non-public warning

Measured decisions

- From 10,000 € Illegal Biometrics (September, 20th 2018)
- To 400.000 € UBER for an attack on the data security of users (December, 20th 2018)

= Few penalties

A spectacular decision, to make an example? CNIL January 21th, 2019

- Google affair – 50 millions euros
- Lack of transparency, unsatisfactory information, lack of prior consent

- 1st application of the new sanction ceilings
- Refusal of the application of the one-stop-shop mechanism

Conclusion: what we can learn from the French example ?

- Still many non-compliant companies
- Impossible use of insurance to guarantee the risk of sanctions (what can be insured?)
- End of the tolerance of the CNIL

Fines imposed by German DPAs

- Results of a survey by a German newspaper*
  - Since May 2018: 75 fines in the total amount of 485,000 EUR.
  - The Baden-Wuerttemberg DPA: total amount of 203,000 EUR in 7 cases
  - In North Rhine-Westphalia: 36 fines

*https://www.welt.de/finanzen/article193326155/DSGVO-Verstoesse-Bundeslaender-ziehen-Bussgeld-Bilanz.html

Fines imposed by German DPAs

- The first fine in Germany: 20,000 EUR against a social media network.
  - Induced by a notification of data breach.
  - Security breach by a cyber attack and the loss of personal data of 330,000 users, mainly passwords and e-Mail-addresses
  - Further investigations by the DPA showed a lack of GDPR required IT security:
    - No hashing of user passwords.
    - Infringement of Art. 32 GDPR.

Further fines imposed by German DPAs

- DPA of Baden-Wuerttemberg: 80,000 EUR – health data were accidently published online. (Art. 9 GDPR)
- DPA of Hamburg: 20,000 EUR – late notification of a data breach and a missing communication to the data subjects.
- DPA of Berlin: 50,000 EUR – unlawful processing of personal data of former costumers by a bank (Art. 6 GDPR).

Fines imposed by German DPAs

- Controversial procedure of the DPAs:
  - Power to investigate without suspicion (e.g. questionnaires by the Berlin DPA) → Is there a right to refuse to give evidence? Even for legal entities?
  - Imposing sanctions because of information transmitted by the companies themselves
    - Especially notifications of data breach (Art. 33 GDPR)
  - Sec. 43 (4) BDSG:

Fines imposed by German DPAs

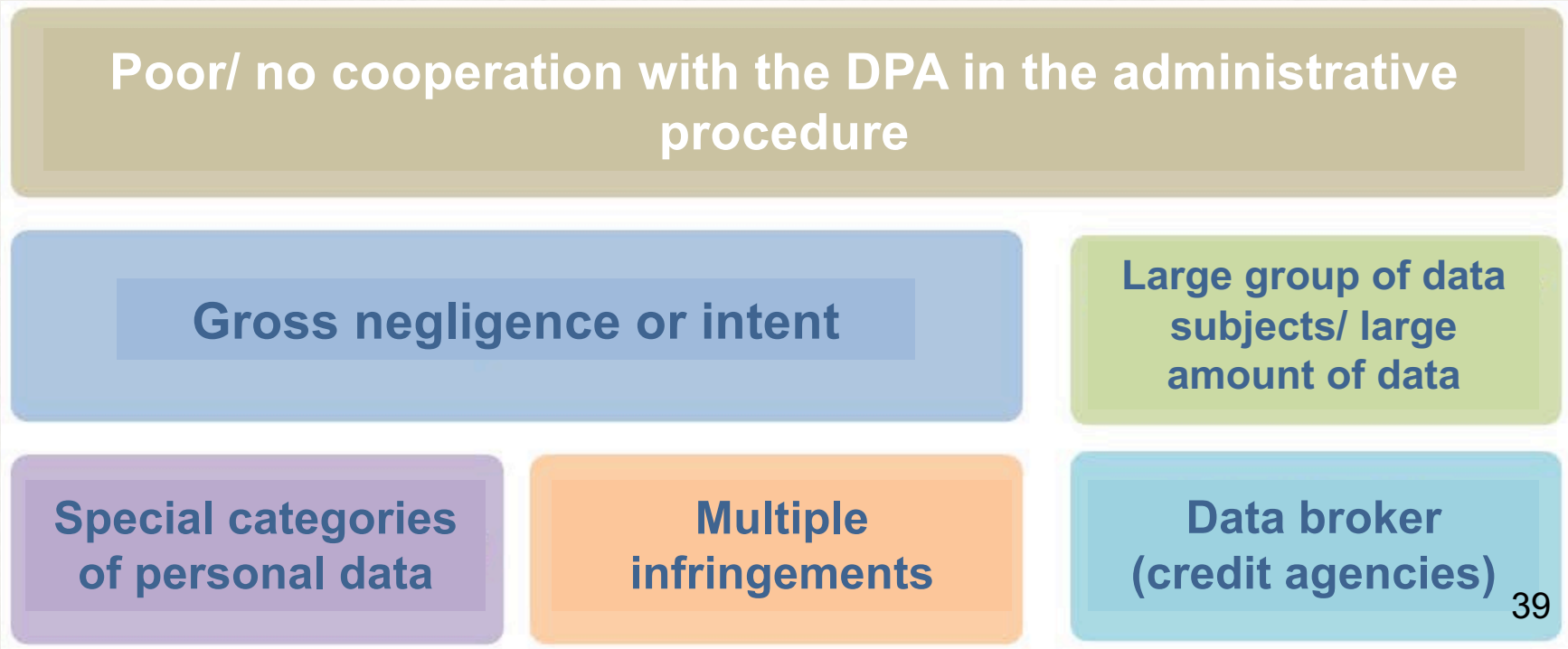
- Sec. 43 (4) BDSG

  A notification pursuant to Art. 33 [GDPR] or a communication pursuant to Art. 34 (1) of [GDPR] may be used in proceedings pursuant to the Administrative Offences Act against the person required to provide a notification or a communication or relatives as referred to in Section 52 (1) of the Code of Criminal Procedure ***only with the consent of the person required to provide a notification or a communication.***

- Baden-Wuerttemberg's DPA: this regulation is contrary to European law.

Fines imposed by German DPAs

- Baden-Wuerttemberg's DPA published criteria for initiation of a fine proceeding in its activity report for 2018:



Retail on DPA‘s focus?

- No sanctions in the retail sector published yet.
- A few investigations:
  - DPA of Bavaria:
    - Offline tracking → Costumer frequency measurement by the Media-Access-Control-Address is a data processing.
      - Only hashed, no anonymized data.
  - DPA of Hamburg:
    - Private retail tracing → Publication of images of alleged thieves from video surveillance systems in shop windows infringes the GDPR.

Insurances and coverages

- DPA of Bavaria (private sector): despite a data protection officer, the **controller** is obliged to comply with the GDPR regulations.
  - DPO shall advise the controller and monitor compliance with this regulation (Art. 39 (1) GDPR).

- Is a self-insured loss coverage for the controller possible?

Insurances and coverages

- In general: no insurance cover for companies against regulatory fines.

- Controversial: regress of fines against the management board.
  - Absorption by a directors and officers (D&O) liability insurance?
  - That does probably not include such encumbrances of assets which are intended to effectively reduce the assets of the company being fined (purpose of the state sanction)

FTC v. Wyndham Worldwide

- Appellate court
  - Upheld FTC's authority to regulate data security "unfair or deceptive acts or practices"
  - Found Wyndham had fair notice that its cybersecurity practices could be subject to scrutiny under FTC Act
- December 2015 settlement:
  - Wyndham to establish comprehensive information security program designed to protect cardholder data – including payment card numbers, names and expiration dates.
  - Wyndham to conduct annual information security audits and maintain safeguards in connections to its franchisees' servers.
  - Obligations continue for 20 years
  - No fine or civil penalty

LabMD, Inc. v. FTC

- Relevant security breaches dating back a decade:
  - 2008 – LabMD billing information for over 9,000 consumers found on a peer-to-peer file-sharing network
  - 2012 – LabMD documents with sensitive personal information of at least 500 consumers were found in hands of identity thieves
- 2013 – After 3-year investigation, FTC filed Admin. Complaint: LabMD failed to adequately protect patient medical data
  - ALJ: FTC failed to demonstrate that it was "likely" consumers had been substantially injured
  - Hypothetical risk of future harm not enough to find LabMD liable for "unfair" conduct under § 5
- FTC reversed; correct inquiry is whether act or practice posed a "significant risk" of injury to consumers
- On appeal, 11th Circuit held in 2018 that FTC's standard language ordering defendants to adopt "reasonably designed" and "comprehensive" data security measures is unconstitutionally vague.

Key Issues in Data Breach Litigation – United States

- Standing
- Damages
- Insurance

Standing

- To have standing, plaintiff has burden of showing:
  - Injury in fact that is
    - Concrete and particularized; and
    - Actual and imminent – not merely conjectural or hypothetical
  - Injury is fairly traceable to defendant's conduct; and
  - Favorable decision is likely to redress alleged injuries
- Actual harm
  - *In re Office of Pers. Mgmt. Data Sec. Breach Litig.* (D.D.C 2017) – unreimbursed expenses for credit repair services = actual injury
  - *In re Yahoo Customer Data Sec. Breach Litig.* (N.D. Cal.2017) – diminution in value of information sufficient
  - *Kuhns v. Scottrade,Inc*. (8th Cir. 2017) – breach of contract confers standing, but no actual injury suffered
  - *Bradix v. Advance Stores Co*. (La. Ct. App. 2017) – two unsuccessful instances of attempted credit fraud insufficient for standing
- Injury based upon actual misuse
  - Payment card or bank account fraud
  - Identity theft
  - Disclosure of medical data or intimate private facts

Standing (continued)

- Risk of future harm
  - Split among Circuit Courts of Appeal
    - 3rd, 6th, 7th and 9th – OK based on risk of future harm
      - *In re Horizon* (3rd Cir. 2017) – 839,000 records, 1 case of misuse
      - *In re Zappos.com Inc.* (9th Cir. 2018) – substantial risk of identity theft
    - D.C. – substantial risk of future harm sufficient
      - *Attias v. CareFirst, Inc.* (D.C. Cir. 2017) – actual unauthorized access
    - 2nd and 4th – reject standing on that basis
      - *Whalen v. Michaels Stores* (2nd Cir. 2017) – 2 attempted charges
- Injury based upon heightened risk of future harm
  - When does risk become "certainly impending" or "substantial"?
  - Risk without actual misuse generally insufficient
- Causation
  - Issue of enablement
    - But consider possibility of data aggregation
  - Denial of data breach
    - *Hutton v. Nat'l Bd. Of Exam'rs in Optometry* (D. Md. 2017)
- Redressability
  - Impact of claim for declaratory or injunctive relief
    - *In re Adobe Systems* (N.D. Cal. 2014)
    - *Dugas v. Starwood Hotels* (S.D. Cal. 2016)

Damages Theories

- Lost time and aggravation
  - *Dieffenbach v. Barnes & Noble, Inc*. (7th Cir. 2018) – lost time / opportunity costs compensable
- Mitigation, prevention or avoidance costs
  - *Sackin v. TransPerfect Glob., Inc.* (S.D.N.Y. 2017) – identity protection service costs
  - *In re Yahoo Customer Data Sec. Breach Litig.* (N.D. Cal.2017) – only those with out-of-pocket mitigation expenditures have cognizable injuries
  - *Savidge v. Pharm-Sav., Inc.* (W.D. Ky. 2017) – fraudulent tax filing not sufficient but prophylactic expenditures are
- Overpayment or "would not have purchased" – *Yahoo* (OK); *Kuhns* (no)
- Intrinsic value
  - No: *Lewett v. P.F. Chang's China Bistro, Inc*. (7th Cir. 2016); In re Sony Gaming Networks Data Sec. Breach Litig. (S.D. Cal. 2012)
  - Yes: *Yahoo* (N.D. Cal.2017) – but purchase required

United States

Insurance Coverage Issues

- CGL policies typically do not cover, even with rider for computer equipment losses
  - CGL policies typically exclude data related losses
  - Rider generally covers 1st party losses, with no obligation to defend 3rd party claims
  - *Innovak Int'l, Inc. v. Hanover Ins. Co.* (M.D. Fla. 2017) – "publication" (covered by policy) is deliberate act, different from negligent data protection
- Cybersecurity policies provide extended coverage, but there are limits
  - *P.F. Chang's Bistro v. Federal Insurance* (D. Ariz. 2016)
    - Defense of class action
    - Forensic investigation into data breach
    - Case management fee
    - Compensation to banks for fraudulent charges/replacements
  - *Columbia Casualty Co. v. Cottage Health* (C.D. Cal. 2015) – misrepresentations and/or omissions of material fact concerning data-breach risk controls
- Business email compromise (BEC) losses
  - *American Tooling Center v. Travelers* (6th Cir. 2018) policy covers money transfer involving fraudulent emails