Cyber Insurance

Insurance against cyber risks

CyberEdge

Insurance against cyber risks

Claims

CyberEdge

Insurance against cyber risks

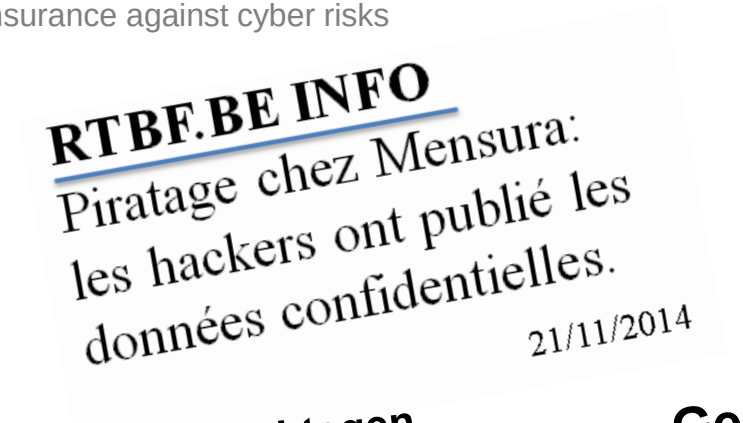
CyberEdge

Insurance against cyber risks

AIG


Hackers stelen klantgegevens bij Domino's Pizza in België en Frankrijk

Belga 13/06/2014


RTBF.BE INFO

Piratage chez Mensura: les hackers ont publié les données confidentielles.

21/11/2014

French TV station TV5 Monde taken off-air by pro-ISIS hack
– 09/04/2015

Opnieuw Cyberaanval tegen website L'Avenir
– Belga - 18/04/2015

Gegevens van 150.000 onderzoeken in Emmaüs-ziekenhuizen onbeveiligd op het net
25/01/16 -16u51 Bron: Belga, ANP


Hackers Leak Details of 6,000 Numericable Customers After Firm Refuses to Pay up

Hackers maken gebruikers populaire datingsite openbaar
– ANP – 22/05/2015

Website Senaat tijd onbereikbaar na aanval
– Belga - 18/05/2015


FINANCIAL REVIEW

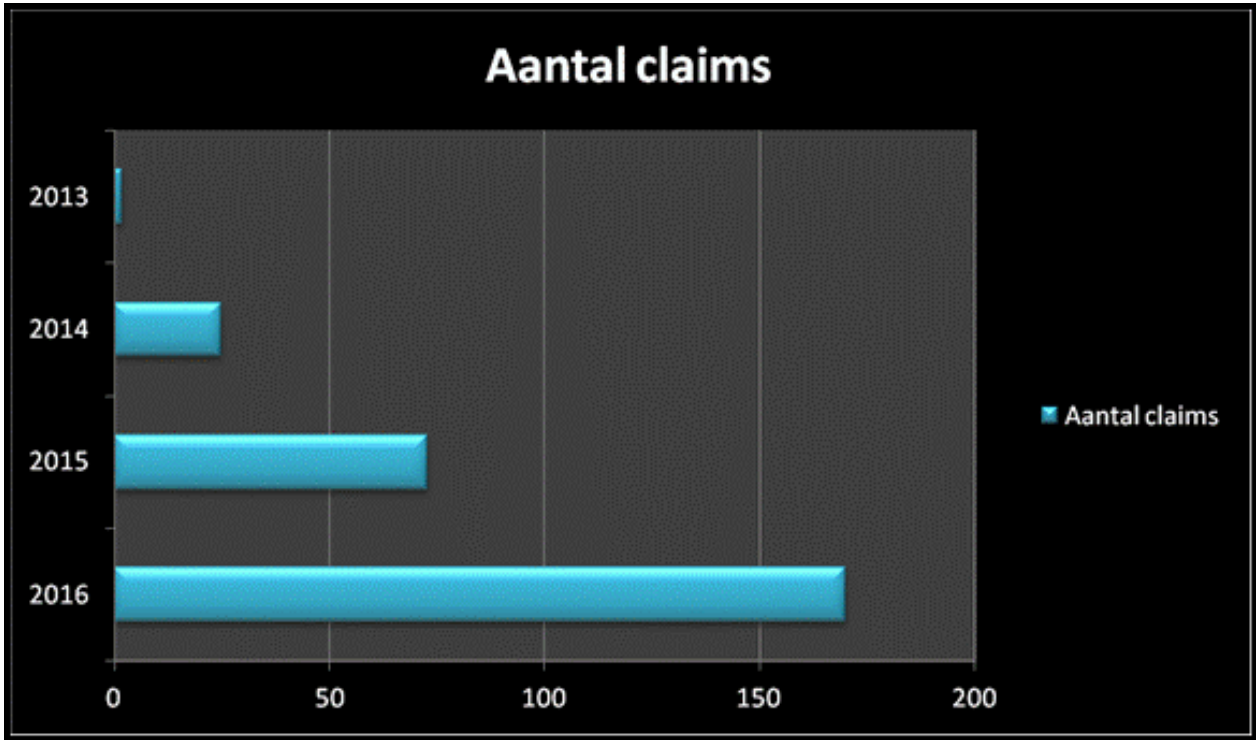
Botnet infected Belgian Charleroi Airport Servers

Ziekenhuis steeds vaker slachtoffer van hacking
11 DECEMBER 2015

CyberEdge

Insurance against cyber risks

Causes of loss

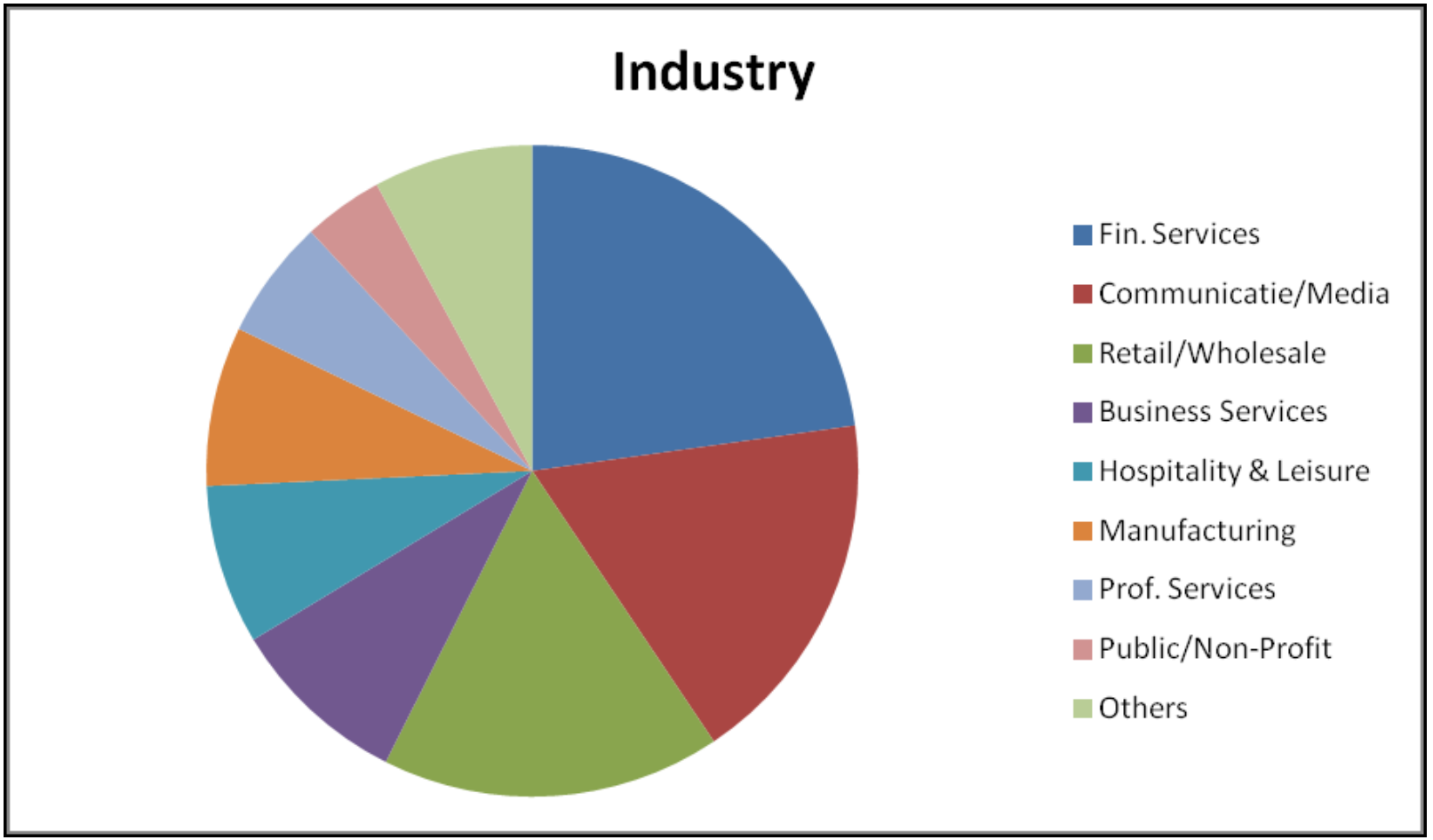


- **EMEA** 2013 – 2016
  - Ransomware: 16%
  - Hacking with data breach: 14%
  - Malware (virus): 10%
  - Data breach: 28%

- **Belgium**: 27 claims
  - Ransomware: 43%
  - Hacking: 10%
  - Malware (virus): 10%
  - 1 Data breach (foreign subsidiary)

Trends

Type sector EMEA



Main concerns

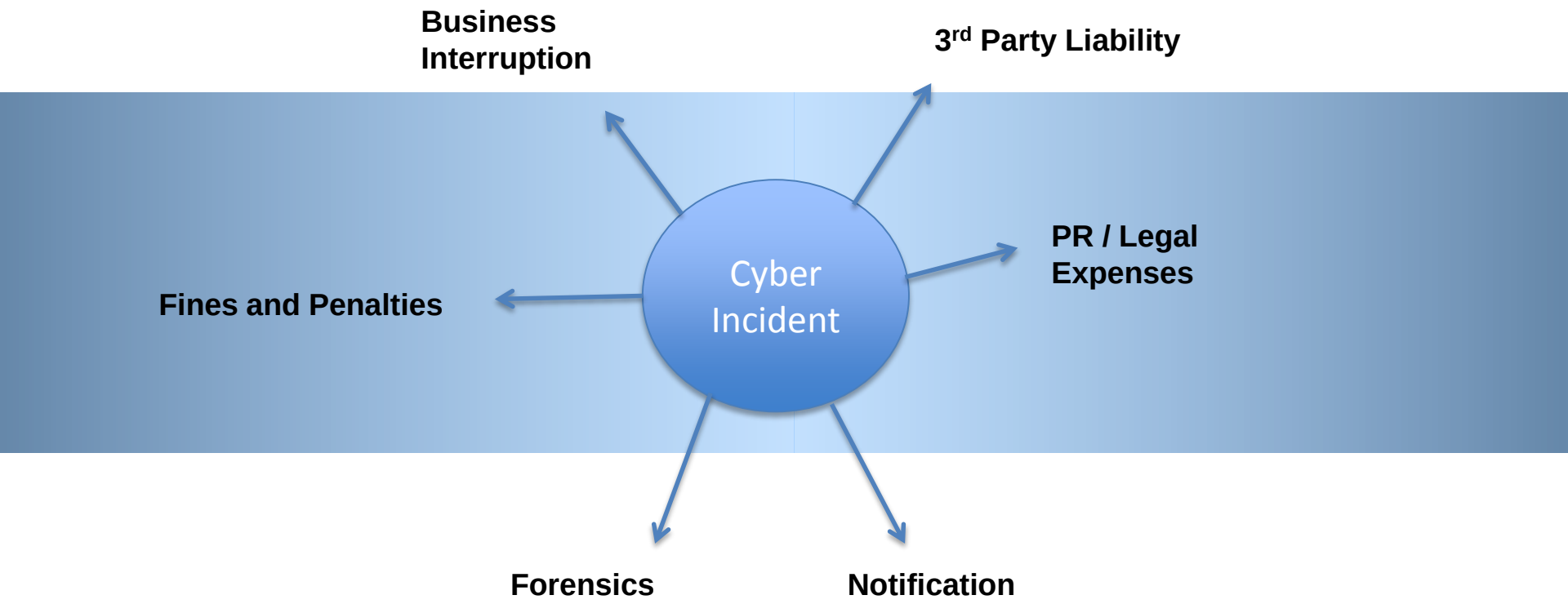
- Former D-Dos extortion; or other type of hacking
- Potential loss of confidential or sensitive info
- Medical liability does not cover privacy issues
- Limited knowledge legal counsel (international!)
- Fear of fines
- Subcontractors
- Contractual obligation
- US-exposure

CyberEdge

Insurance against cyber risks

Policy

Cyber Exposures



Coverages

Event Management

Liability / Legal Defense

Other coverages:

- **Media Content Liability**
- **Cyber Extortion**
- **Cyber Theft**
- **Telephone Hacking**

Data Protection obligation

Network business interruption

- Fraud/fidelity but intentional acts: yes
- Property damage
- Physical cause
- Loss of goods (except Cyber theft)
- Reputational damage
- Systems

CyberEdge

Insurance against cyber risks

Underwriting

CyberEdge

Insurance against cyber risks

Criteria

- Data - activity
- Security
- Geography
- Claims
- Limit /deductible

Underwriting - Hazard Classes

LOW RISK	Manufacturing, Wholesale, Warehousing and Construction
MEDIUM RISK	Retail, Transportation, Education, Entertainment, Real Estate and Professionals (HR!)
HIGH RISK	Telecommunications, Medical, Internet Services, Data Processing, Telemarketing and Media, Retailers, Credit Bureaus, Payment Processors, Gaming Companies , Social Networking Firms, Cloud Providers
VERY HIGH RISK	Financial institutions

- Property?
- Casualty?
- Professional liability?
- D&O?
- Crime?
- Kidnap & Ransom?

CyberEdge

Insurance against cyber risks

Conclusion

CyberEdge

Insurance against cyber risks

Conclusion

- Absolute need for business continuity
- Not just an insurance! Service is key
- Any firm is a target
- Fast growing

Cross-border data transfers: rules & restrictions

Héloïse Bock

17/05/2017

Event organized by:

AMCHAM LUXEMBOURG
AMERICAN CHAMBER OF COMMERCE IN LUXEMBOURG A.S.B.L.

Introduction:
Key challenges in relation to cross-border data transfers

- Differences in approach to privacy protection across the world

- GDPR→ large territorial & material scope and applies to:

  - EU-based DC or DP and (in certain cases) DC or DP not established in the EU (e.g. when data processing targets European customers)
  - All DC or DP which process personal data relating to an identified or identifiable natural person

  e.g. account number, IP address, e-mail address of contact person within a company

- Cross-border data transfers would normally imply the following elements: ”*communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it*” (EDPS).

Basic principles surrounding data transfers

- Data transfers within the EU

Free, bear in mind:

- must comply with the principles of the data protection legislation (adequacy, necessity, and proportionality etc.)

- Data transfers outside of the EU

Prohibited unless:

1. the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
2. the data exporter puts in place appropriate safeguards; or
3. a derogation or exemption applies.

Adequacy decision & appropriate safeguards

1. The jurisdiction ensures an adequate level of protection

- Ruling of the European Commission (regular re-evaluation)

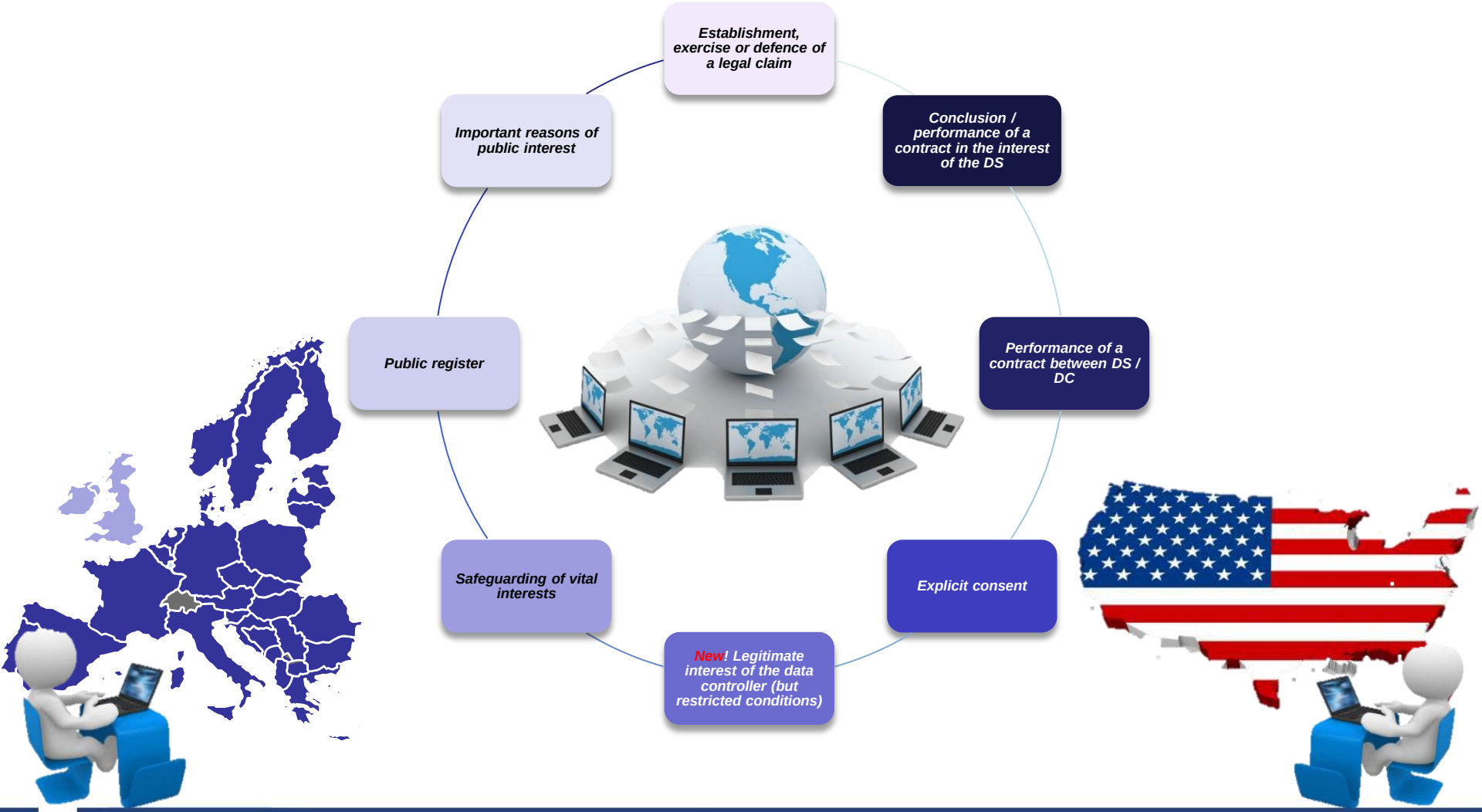
- Jurisdictions currently ensuring an adequate level of protection:

  Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay

2. Transfer on the basis of appropriate safeguards

(in the absence of adequacy decision)

3. If one of the legal exceptions applies



How to legitimate data transfers to the USA?

- Schrems ruling handed down in October 2015 (C362/14)
  - ✓ CJEU invalidated the Safe Harbor agreement which allowed data transfers where US recipients voluntarily agreed to meet EU standards

- "EU-US Privacy Shield" adopted in July 2016
  - ✓ Stronger obligations on U.S. companies to protect Europeans' personal data compared to Safe Harbor
  - ✓ Sufficient?
  - ✓ Criticisms point out:
    - G29: "Massive and indiscriminate" bulk collection of EU citizens' data by US authorities
    - Failure to provide express data retention provisions
    - Significant improvements required by G29 and EDPS (e.g. ombudsman to handle complaints from EU citizens, annual review by the EU and US etc.)
  - ✓ Already challenged by Irish and French privacy advocacy groups before the ECJ

Uncertainty surrounding data transfers to the USA

- EU standard contract clauses
  - ✓ Challenged by Irish DPA before the ECJ since:
    - Do not prevent mass surveillance by U.S. intelligence authorities
    - Do not offer suitable redress to EU citizens whose rights have been impinged

- Binding Corporate Rules?
  - ✓ Only for multinational group of companies which define a global privacy policy
  - ✓ Same problems as EU standard contract clauses

- Consent?
  - ✓ From unambiguous (Directive) to explicit consent (GDPR) → data subject must "respond actively to the question, orally or in writing" (Article 29 WP)
  - ✓ But:
    - Expensive and takes time
    - Not an adequate basis in many cases (e.g. mass transfers of personal data)
    - Can be withdrawn at any time

Tough sanctions in case of violation of the data transfer provisions

- Maximum fines of up to 4% of global turnover or € 20 M
- Directly applicable by the supervisory authority
- Other sanctions: ban on processing, order to erase data, etc.

Contact us

- **Héloïse Bock**
  - Partner at Arendt & Medernach
  - Member of the Council of State
  - Tel : +352 40 78 78 321
  - Email : Heloise.Bock@arendt.com

EU General Data Protection Regulation (GDPR)

Amcham – Take control of your risk

Risk Management

17/05/2017

Building a better working world

Your Contacts

Olivier Maréchal
Partner | Advisory leader

Tel :+352 42 124 8948
Mobile :+352 621 838 948
E-Mail Olivier.marechal@lu.ey.com

Francois Barret
Senior Manager – Data Privacy & Cybersecurity Leader

Tel :+352 42 124 8547
Mobile :+352 621 838 175
E-Mail francois.barret@lu.ey.com

Content

- Risk-based approach
- Risk
- Data Privacy Impact Assessment
- Third party management
- International Transfers

Risk-based approach

- Risk Assessment are required under EU Data Protection Directive
- However, GDPR broadens the relevance of risk, as it is explicitly based on the notion of **risk-based approach:**
  - Effective tool for ensuring protection of the rights and freedoms of individuals
  - Helps devise effective and appropriate mitigations and controls, by assessing the likelihood and significance of the impacts and any potential harms to individuals
  - Enables organization to prioritize tasks and allocate their resources effectively towards compliance

High-risk processing

GDPR introduces stricter requirements for high-risk processing:

Activities	Additional Obligations	Exemptions
• **Systematic and extensive automated profiling** • **Large-scale processing of special categories of data** • **Large-scale, systematic monitoring of a publicly accessible area** • **Other activities that are "likely to result in a high risk for the rights and freedoms of individuals"** • **Member state law**	Privacy impact assessments	Member state law exempts specific activities
	Prior consultation with DPA	Controller implements appropriate technical and organizational measures to mitigate the risk
	Notification of data breach to individuals	• Controller implements appropriate technical and organizational measures (e.g. encryption) • The high risk is no longer likely to materialize • Notifying affected individuals would involve disproportionate effort

Not High-Risk processing

For activities that are not tagged high-risk, controllers still must adopt measures that are appropriate to the risk level of the activity:

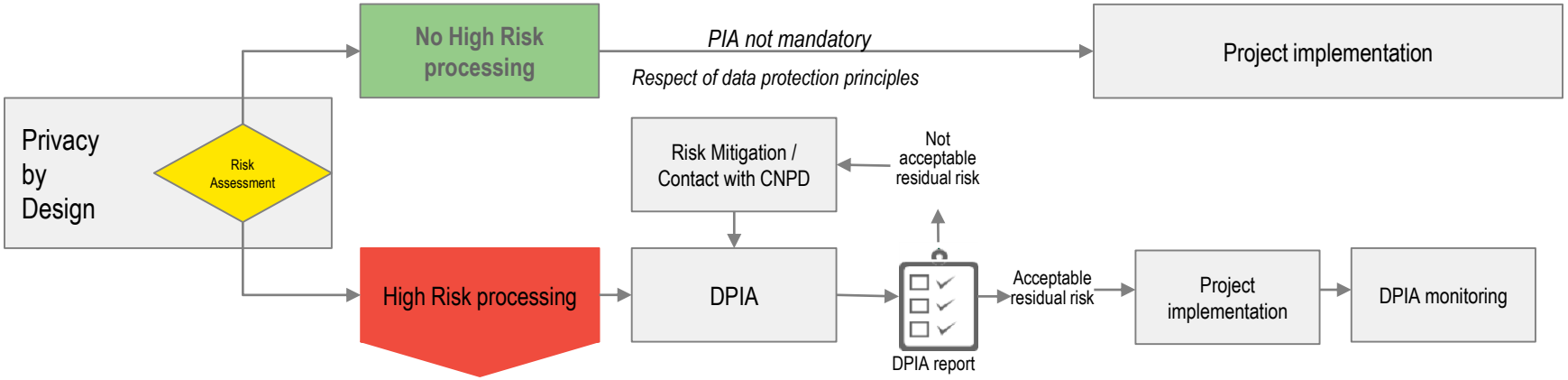
Activities	Additional Obligations	Exemptions
Examples • Data subjects deprived of control • Processing sensitive data • Profiling • Vulnerable individuals • Large-scale processing Potential Harms • Discrimination • Identity theft or fraud • Financial loss • Damage to the reputation • Loss of confidentiality • Reversal of pseudonymization • Significant economic	Notification of data breach to DPA	Data breach is "unlikely to result in a risk for the rights and freedoms of individuals"
	Foreign controllers appoint EU representative	Processing is occasional, does not include large-scale processing of sensitive data, *and* is "unlikely to result in a risk for the rights and freedoms of individuals."
	Data security: Controllers must implement (and choose processors that implement) "technical and organizational measures" appropriate to the risk of a data breach	Controller processes only "anonymous data" not subject to regulation
	Risk-based compliance with GDPR's "general obligations"	Controller processes only "anonymous data" not subject to regulation

Data Privacy Impact Assessment (DPIA)

High level description

High level principle	Article 35

- PIA is a method designed to identify and evaluate **risks arising from data processing**, in order to carry out the adequate measures to mitigate them. PIAs also contribute to **demonstrate Privacy by design principles are in place**.
- To perform PIA, Responsible for data processing should **identify processing** applied to data, their **purpose** and their **level of risk**
- Responsible for data processing should perform **PIA** if processing poses **high risk** regarding data subject's **rights and freedoms**



To date, 3 cases where **PIA** must be performed by default are mentioned by GDPR (c.f. Article 35, §3):
1.Automated **decision making or profiling**
2.Processing on **sensitive data** and personal data relating to **criminal convictions**
3.Monitoring of a publicly accessible area on a **large scale**
*This list will be **enriched by CNPD***

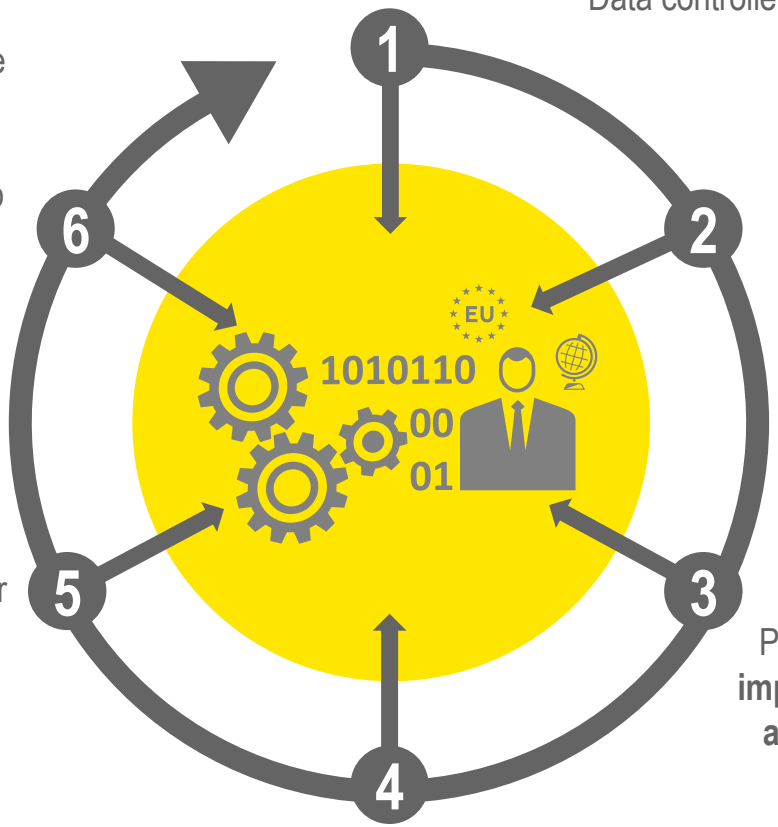
- Privacy Impact Assessment allows to identify measures to **mitigate risks**, decreasing their **probability** or **gravity**.
- It also allows to assess risks (origin, type, impact, …)

PIA results must allow to determine the appropriate means to set-up to demonstrate how far this process is GDPR compliant

Third party management
Data Processors (new) obligations

Data processors (new) obligations

1. Enter into a **written agreement** with the Data controller
2. **Jointly responsible** with the Data controller and appointment of a data protection responsible
3. Provide sufficient guarantees to **implement appropriate technical and organizational measures**
4. Carry out **Privacy Impact Assessments (PIA)**
5. **Notify the controller of a personal data breach** without undue delay after becoming aware of such breach
6. **Maintain documentation** about the processing operations carried out and submit the documentation to a supervisory authority if requested to do so



International Transfers
Cross-border data transfer

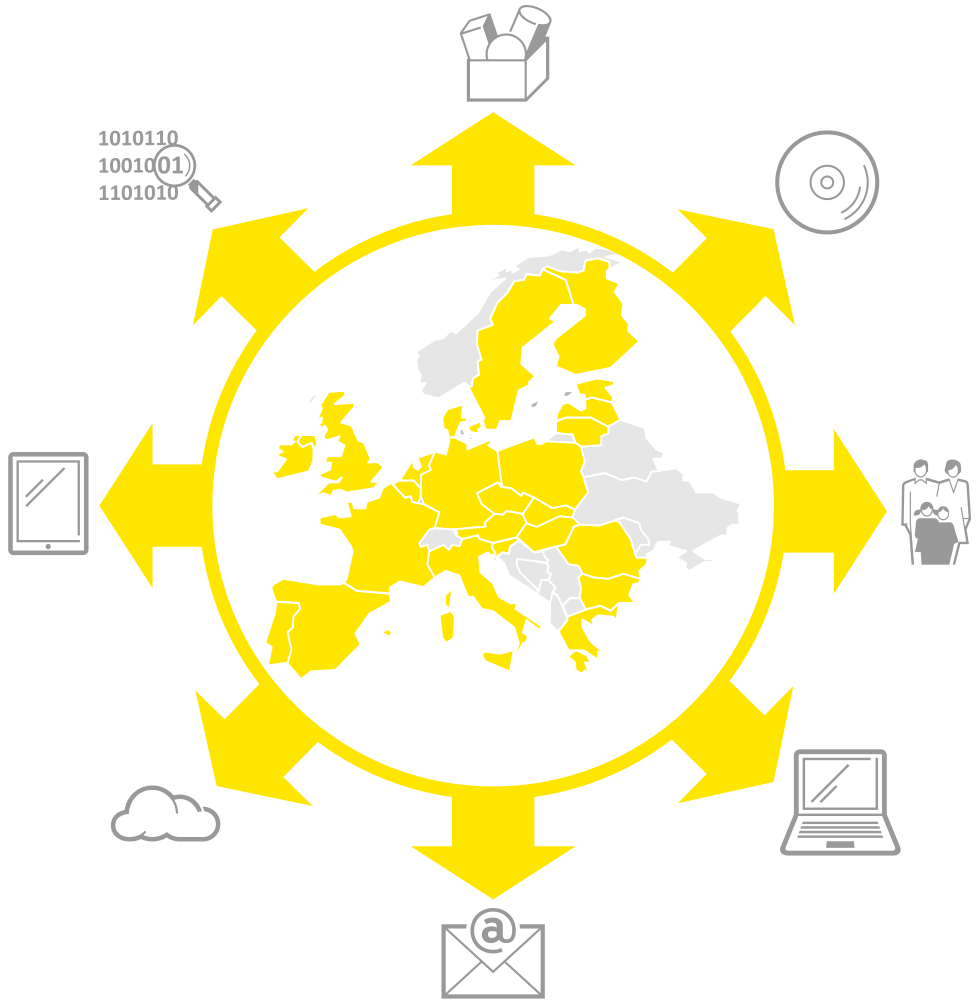
Cross-border data transfer

GDPR permits personal data transfers to a third country or international organization subject to **compliance with set conditions**, including conditions for onward transfer.

GDPR allows for data transfers to countries whose legal regime is deemed by the EU to provide an **adequate level of personal data protection**.

Transfers outside the EU are **allowed if appropriate safeguards are in place**, such as

- Standard contractual clauses
- Binding corporate rules (BCRs)
- Approved code of conduct or certification mechanism (e.g. “European Data Protection Seal”)



EY

Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 213,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

EY refers to the global organization of member firms of EY Global Limited, each of which is a separate legal entity. EY Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

www.ey.com/luxembourg

Building a better working world