



Are you and your organization ready for GDPR?

PMI Belgium Chapter Event 19 April 2018 at ISF Tervuren



Agenda

- 18:30 – 19:00 Registration
- 19:00 – 19:15 Welcome Message & Introduction
- 19:15 – 20:15 Presentation on GDPR
- 20:15 – 20:45 Panel on GDPR
- 20:45 – 21:30 Closing words, Networking & Refreshments



19:00 – 19:15

Welcome Message & Introduction

Chapter Events

- Tuesday 5th of June – AE, Architects for Business & ICT
 - Theme: “Are you ready for a mysterious business game?”
 - Format: Challenging business interactive game where collaboration and communication are key.
 - Venue:
AE - Architects for Business & ICT
Interleuvenlaan 27b
3001 Heverlee
Belgium
 - Registration will open 20th of April

Satellite Events

- Tuesday 29th of May - @CMAST - Temse
- Thursday 7th of June - @Mölnlycke Health Care - Waremmme

PMFair

- Date: Friday 5th of October 2018
- Theme: Facilitation: The Ultimate PM Skill?
- Venue: Proximus Lounge – rue Stroobantsstraat, 51 – 1140 Evere (Brussels)
- Format: presentation in a TEDx format and in parallel Market Place (called Inspiration Hall).

Inspiration Hall

- The Inspiration Hall will have 20+ stands, 1 premium stand (4X normal stand) and 2 activity areas, where the debates, skill workshops, ... will be held.
- In order for the Inspiration Hall to be a success, both stand holders and non-stand holders have to participate actively



Inspiration Hall

- Centred on 4 main experiences:
 - Learning new skills
 - Engaging in discussions
 - Meeting new People
 - Finding a new challenge
- Contact: events@pmi-belgium.be

one extra
networking opportunity
for your attendance in
Chapter event
carpooling



- We have launched the Carpooling initiative this year to help our members.
- The success of this initiative will depend on your participation.
- Carpooling is not only beneficial to those who do not have the convenient means of transportation, it is also a way to help our environment and to increase your network.



BELGIUM CHAPTER
20 Years 1998-2018





19:15 – 20:15

Presentation on GDPR

General Data Protection Regulation



19 APRIL 2018

© Kris Troukens – GeDaPRe.eu - kris.troukens@gedapre.eu



facebook



amazon

Explosion of Data

GPS

Google

Amazon

Facebook

Apple

Privacy?

1995

Latest directive
on Data
Protection



Nearly Half of the Norway Population Exposed in HealthCare Data Breach

Sunday, January 21, 2018 Swati Khandelwal

Share 3.11k

Norway

Massive HealthCare Data Breach



Cybercriminals have stolen a massive trove of Norway's healthcare data in a recent data breach, which likely impacts more than half of the nation's population. An unknown hacker or group of hackers [..

Nearly 2000 WordPress Websites Infected with a Keylogger

Monday, January 29, 2018 Swati Khandelwal

Share 1.42k



More than 2,000 WordPress websites have once again been found infected with a piece of crypto-mining malware that not only steals the resources of visitors' computers to mine digital currencies but

Vulnerability in Hotel WiFi Network Exposes You to Hackers

Thursday, March 26, 2015 Swati Khandelwal

Share



Ransomware Hijacks Hotel Smart Keys to Lock Guests Out of their Rooms

Saturday, January 28, 2017 Mohit Kumar

Share



Ransomware Locks Down Hotel Rooms

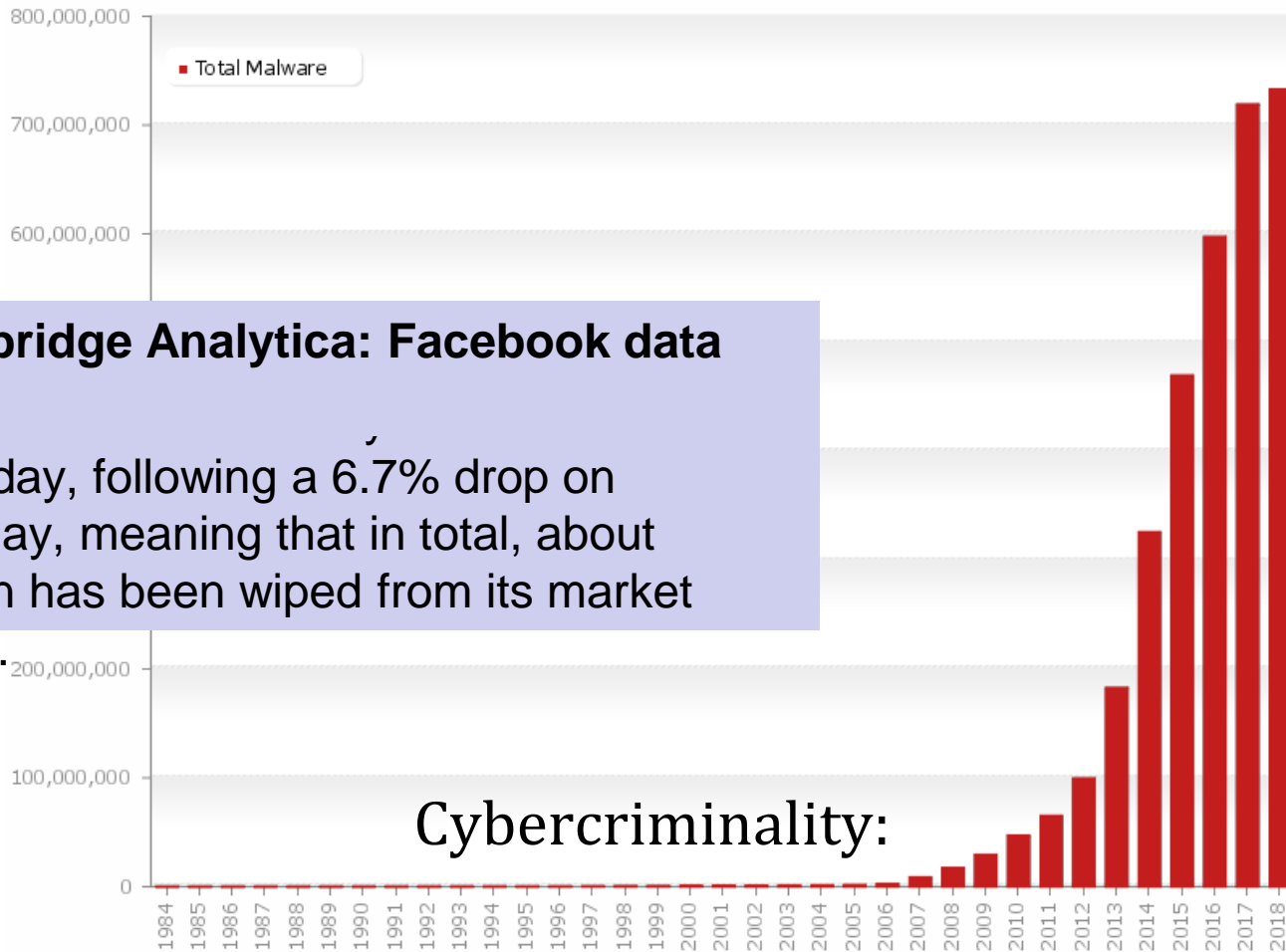
Hackers Steal Payment Card Data From Over 1,150 InterContinental Hotels

Wednesday, April 19, 2017 Swati Khandelwal

Share



Explosion of DATA BREACHES



Cambridge Analytica: Facebook data row

Tuesday, following a 6.7% drop on Monday, meaning that in total, about \$50bn has been wiped from its market value.

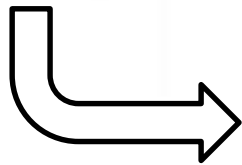
Cybercriminality:

Last update: 02-01-2018 11:52

Copyright © AV-TEST GmbH, www.av-test.org

Some Facts:

1. Fact : we all THINK we are in control of our personal data
2. Fact : this personal data is NOT properly protected
3. Fact : Society has dramatically evolved since 1995
4. Fact : « EU Agenda DIGITAL 2020 »
Ambition to make Europe the center of excellence of Information Technologies by 2020
This requires efficient and effective control of personal data



NEW DIRECTIVE

PITFALLS !

1. Involve Legal Council



Today



28 interpretations of the
1995 Directive



Tomorrow



1 Regulation,
applicable in all
member states

Territorial scope



Established in the EU / Concerning EU citizens

Applies **worldwide** to whoever sells goods or services to EU citizens

PERSONAL DATA



Personal Data

Name
Birthdate
Address
IP
Picture



Sensitive Personal Data

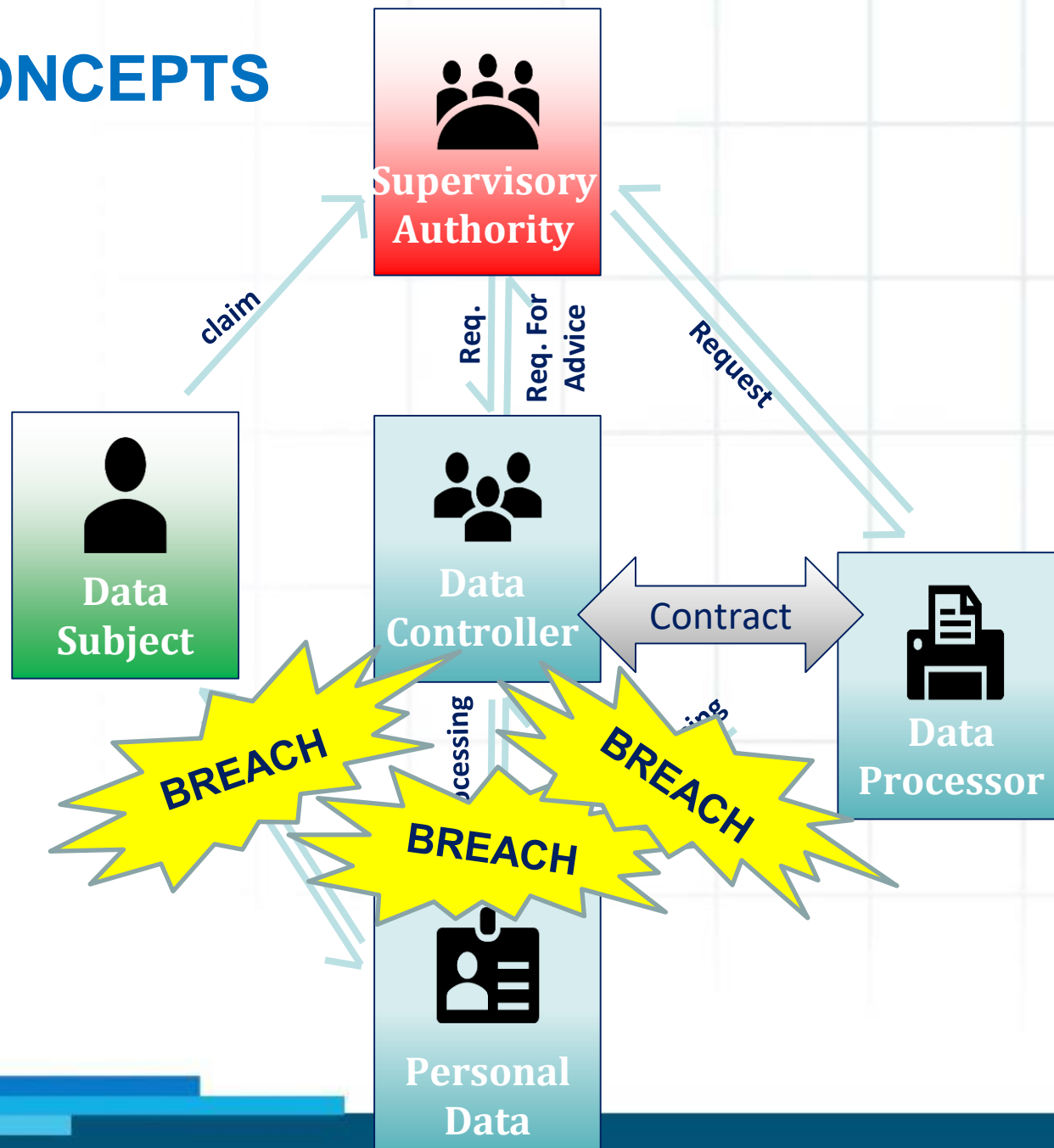
Race
Ethnicity
Sexuality
Philosophical
Trade Union
Health



Genetic & Biometric Data

Gene Information
Fingerprints
Facial Recognition
Retina scans

KEY CONCEPTS



PITFALLS !

1. Involve Legal Council

2. Start with an inventory of your BP



Data Subject Rights

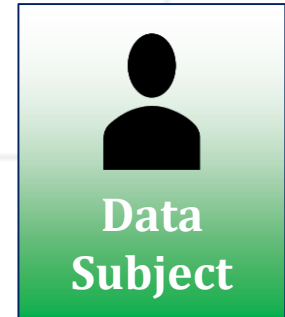
- 1. The right to access*
- 2. The right to be forgotten*
- 3. The right to data portability*
- 4. The right to be informed*
- 5. The right to have information corrected*
- 6. The right to restrict processing*
- 7. The right to object*
- 8. The right to be notified*



***Are you
prepared?***

DATA SUBJECT RIGHTS :

- Right to be informed
- Right of access
- Right of rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to manual processing



Lawfulness [*Legalité*]

- For the performance of a contract
- Person has given his consent
- Legal obligation
- To protect vital interest of a person
- Public interest
- Legitimate interest

Hotel sells a room

I agree that you use my data

I need your data to pay salary

Unconscious

Voters register

Hospital contacting arthrosis patients



- If one of these conditions is met, the processing is lawful



CONSENT

He makes the reservation himself (time of reservation)

He ticks a box upon arrival (I agree that you process my data)

If I don't have
an **EXPLICIT**
"YES"
then it's a
"NO"

Consent Given	How	Date Given	Date Withdrawn
<input checked="" type="checkbox"/>	PMS	27/03/2014	
<input checked="" type="checkbox"/>	RegCard	01/01/2018	01/03/2018

Ideally automated ...



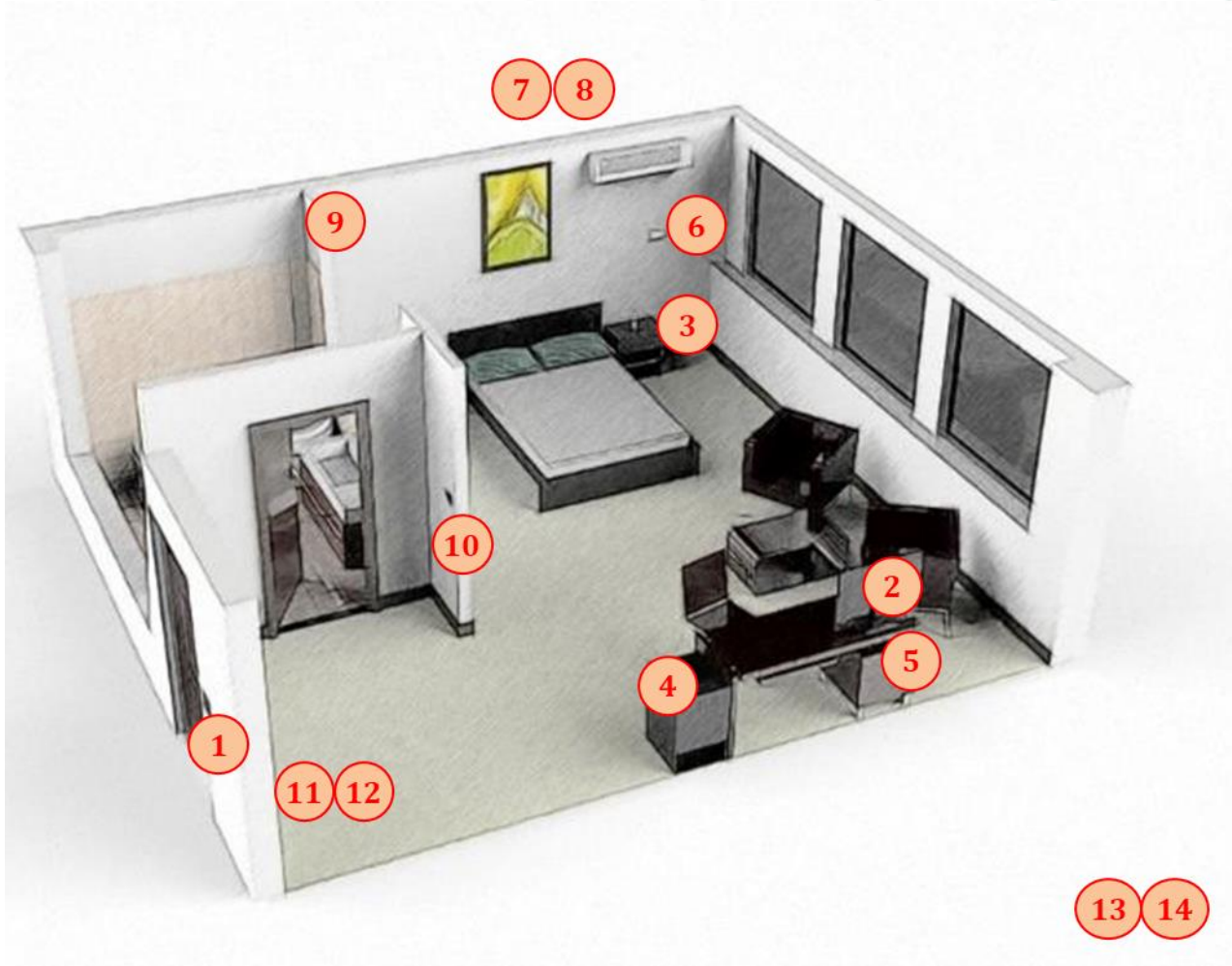
EXERCISE HOTEL-ROOM



**Identify all
possible DATA
flows**

IN ROOM

- **Validate Contracts with subcontractors**



1. Door Lock
2. TV
3. Telephone
4. Minibar
5. Safe
6. Climate/energy control
7. Firealarm
8. Sprinkler
9. Motion detector
10. Light switches
11. DND switch
12. HK switch
13. WI-FI
14. CONTRACTS

PITFALLS !



1. Involve Legal Council
2. Start with an inventory of your BP
3. Think about shadow systems

- 1** **CREATE AWARENESS**
- 2** **CREATE GDPR REGISTERS**
- 3** **COMMUNICATE TO YOUR CUSTOMERS**
- 4** **RISK ANALYSIS**
- 5** **PROCEDURES**

1 Late awareness

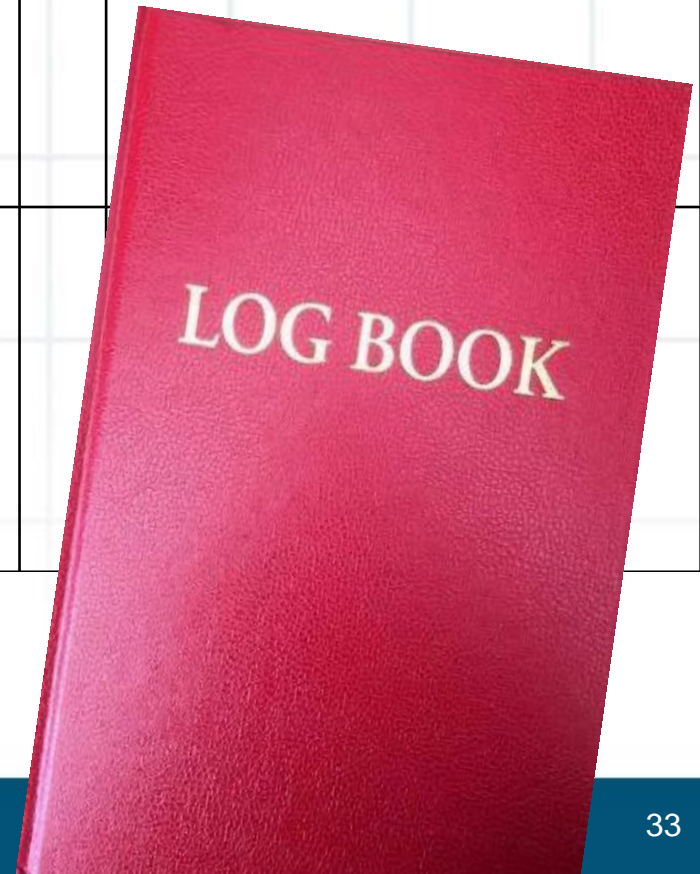
	Deliverables
Inform entire company	Awareness session PPT

A lot of information exists
Presentations exist :

Commission de la vie privée www.privacycommission.be
Privacy commission
Commissie bescherming persoonlijke levenssfeer

2 Date GDPR registers

	Deliverables
This LOG (« Bible ») should contain all steps taken by the hotel during the preparations and on-going phases leading up to May 2018	Register(s)
<ul style="list-style-type: none">• GDPR Logbook• Register of processing activities - Processes• Contracts Register• Risk Register	
In future Will also include <ul style="list-style-type: none">• Data Subject requests• Breach notifications	



EXAMPLE “GDPR LOGBOOK”

DATE	WHAT	EXPLANATION - DECISION	REF
01 03 2018	Introduction to GDPR	Session d’info par VisitBrussels	visit.brussels
	Start of Logbook		
	Audit		
	Plan d’action		
		

REGISTER OF PROCESSING ACTIVITIES

- Start by listing your processes
- Think about all SYSTEMS
- Think about all DEPARTMENTS
 - HR example :
 - Hire new employee
 - Pay salary
 - Perform annual evaluation
 - Dismiss employee
 - Marketing / Conferences / IT / Engineering

REGISTER OF PROCESSING ACTIVITIES

- If we have the right processes, we can derive the data processing :
- The list will start to grow :

	Process	System	Brand/Version	Data Type	Contains Pers Data	Purpose	Reason	Interfaces	Supplier	Contract	Consent Captured	Technology
Pay Salary	Partena	V1.6	Personal	Y	Salary admin	Contractual obligation	Y	Partena	Y	N	web	

PITFALLS !



1. Involve Legal Council
2. Start with an inventory of your BP
3. Think about shadow systems
4. Don't rush to encrypt everything

3 Communicate to your customers

		Deliverables
Create / Amend existing Privacy Policy		WEB
Are all rights of the customer mentioned ?		
How can the customer request access :		<ul style="list-style-type: none"> • Procedure to handle this • Procedure to remove data • Procedure to communicate data electronically

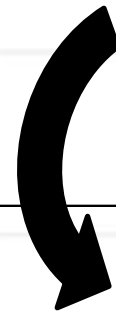
Good example of Privacy Policy

ACCOR HOTELS
First Welcome

CUSTOMER PERSONAL DATA PROTECTION CHARTER

1. The AccorHotels Group's commitment to protecting privacy
2. Consent
3. AccorHotels's seven principles for protecting your personal data
4. Scope of application
5. What personal data is collected?
6. When is your personal data collected?
7. For what purposes?
8. Conditions of third-party access to your personal data

9. Protection of your personal data during international transfers
10. Data security
11. Cookies
12. Storage of data
13. Access and modification
14. Updates
15. Questions and contacts



- Need to be written
- Need to be trained

Register of contracts

- What should go in this register ?
 - **System / Supplier**
 - **Date of the contract**
 - **Document reference / version**
 - **Deals with Personal Data ?**
 - **Paragraph on GDPR ?**

4 ANALYSIS

What can go wrong with the data ? What can go wrong with the system ? Are the systems ready ? Is there anything that can be done about it ?		
The company is responsible for the SAFE and SECURE processing of the Personal DATA		



RISK REGISTER

- Continue to build

Data Risk	Probability	Impact	Technology Risk	Probability T	Impact T	RISKSCORE
	H	M		H	M	2
						4
						6

Scoring allows you to SORT your risks by importance
HIGH risks should be worked on ...

1

CREATE AWARENESS

2

CREATE GDPR REGISTERS

3

COMMUNICATE TO YOUR CUSTOMERS

4

RISK ANALYSIS



ACTION PLAN

Task	Start Date	End Date	Progress	Responsible
1. Create Awareness	2023-01-01	2023-01-15	100%	John Doe
2. Create GDPR Registers	2023-01-16	2023-01-30	50%	Jane Smith
3. Communicate to your customers	2023-01-31	2023-02-15	20%	John Doe
4. Risk Analysis	2023-02-16	2023-02-28	10%	Jane Smith

5 Procedures

	Deliverables
Guest Requests : <ul style="list-style-type: none">• Right to know• Right to obtain a copy of his data• Right to correct his data• Right to be forgotten	Procedures Reply within 1 month
Data Breach Procedure	Procedure to detect Procedure to notify authority Procedure to notify Guest Report within 72 hrs



- Need to be written
- Need to be trained

PITFALLS !



1. Involve Legal Council
2. Start with an inventory of your BP
3. Think about shadow systems
4. Don't rush to encrypt everything
5. Do you have GDPR skills

- 1 CREATE AWARENESS**
- 2 CREATE GDPR REGISTERS**
- 3 COMMUNICATE TO YOUR CUSTOMERS**
- 4 RISK ANALYSIS**
- 5 PROCEDURES**



More complex program

1 RAISE AWARENESS

- Staff Training / Awareness
- Most breaches due to lack of awareness
- = start of the mitigation
- GDPR Program Logbook
- Inform Customers : Access Requests / Privacy Policy / Cookies ...

2 REVIEW POLICIES & RELATED DOC

- Review existing policies
- Create new policies
 - Rights of the guest / age
 - Data breach
- Train your staff
- How do you capture Consent

- Consent Register
 - Manual/electronic
- Policy Refresh

3 IDENTIFY & SCORE RISKS

- Risks related to how process Data
- Contracts with suppliers
- Compile a risk Register

- Risk Register
- Contracts Register

4 CONDUCT AN AUDIT

- Know your data
- How you got it / who can access / where stored / how long / shared with
- Legal Basis

- Data & Process Register

5 PLAN & EXECUTE

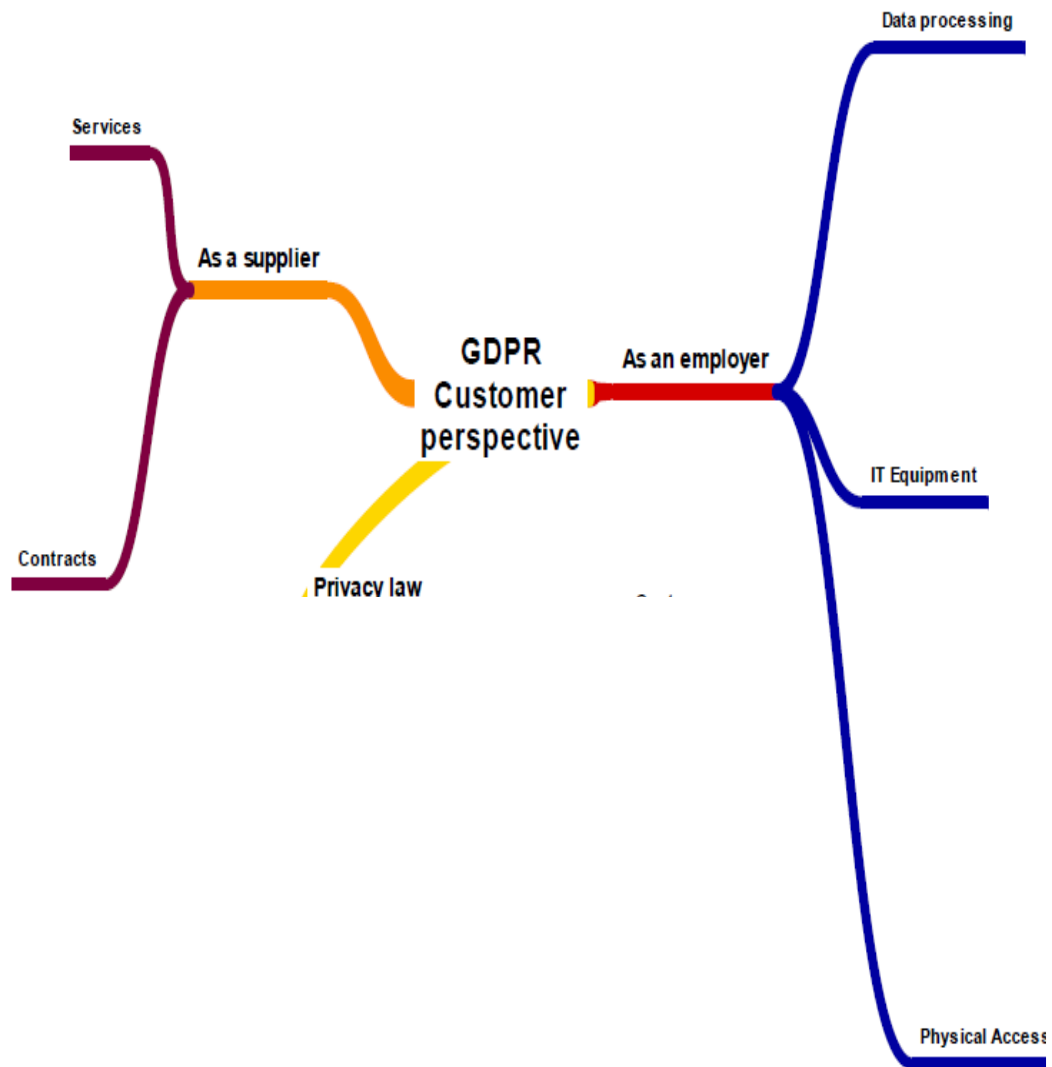
- Determine your roadmap to compliance
- Execute the plan
- Design Data Privacy
- International ?

- Plan + deadlines
- Execution
- DPO ?

6 REVIEW PERIODICALLY

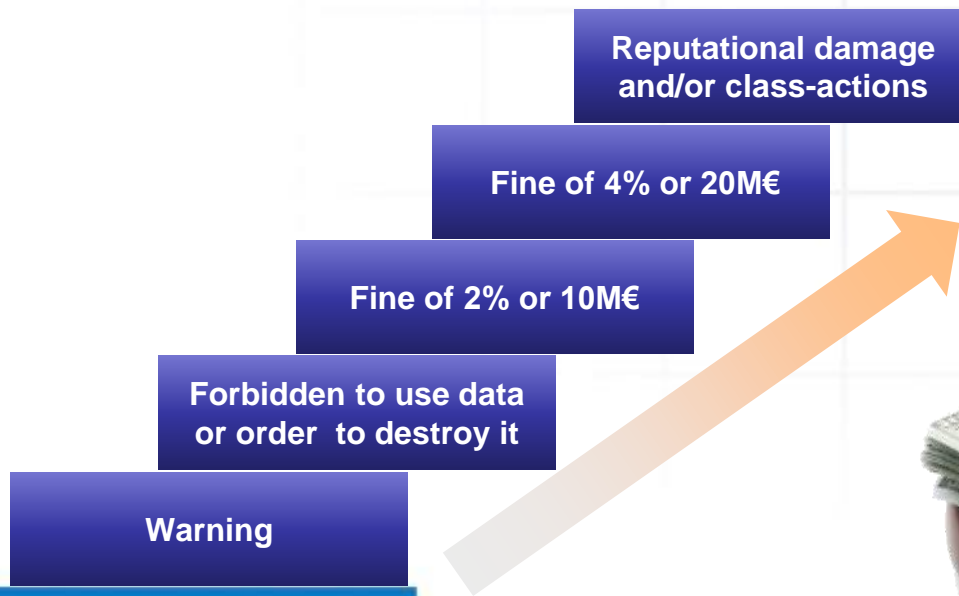
- Get into the habit of doing regular checks and updates
- All of the above still up-to-date .

- Review on a regular basis : People and systems change



!alties

Fines of up to 20 million € or 4% of annual global turnover , whichever is the greatest		
Turnover is total (GROUP) SALES		
Example		100 million € = 4 million €





kris.troukens@gedapre.eu



20:15 – 20:45

Panel on GDPR

GDPR PANEL

- **Panel members:**
 - Xavier Darmstaedter – Partner GeDaPRe.eu
 - Kris Troukens – Partner GeDaPRe.eu
 - Christophe Balduck – Data Trust Associates
 - Stijn Muylle – Falcon Projects
- **Moderator:** Frank Turley



20:45 – 21:30

Closing words, Networking & Refreshments

Closing words

- CoP → Frank Turley

Networking & Refreshments

