

General Data Protection Regulation

GDPR
GENERAL
DATA PROTECTION
REGULATION

AVG
ALGEMENE
VERORDENING
GEGEVENSBECHERMING

RGPD
REGLEMENT GENERAL
SUR LA PROTECTION DES
DONNEES

AGENDA



General
Data
Protection
Regulation

- Introduction
- Law & Background
- Basic concepts & Legal Ground
- What does this mean in a hotel/museum/tourist office ...
 - Some changes in preparation
 - Prepare for questions later

PRACTICAL

PRACTICAL

PRACTICAL



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 Share Tweet Share

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 [...]

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

Saturday, January 28, 2017 Mohit Kumar

Share Share Tweet Share Share Mail Share



Nearly 2000 WordPress Websites Infected with a Keylogger

Monday, January 29, 2018 Swati Khandelwal

Share 1.42k Share Tweet Share



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 [...]

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

Wednesday, April 19, 2017 Swati Khandelwal

Share Share Tweet Share Share Mail Share



Vulnerability in Hotel WiFi Network Exposes You to Hackers

Thursday, March 26, 2015 Swati Khandelwal

Share Share Tweet Share Share Mail Share

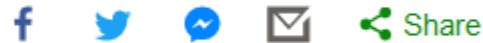


EXPLOSION OF DATA BREACHES

Technology

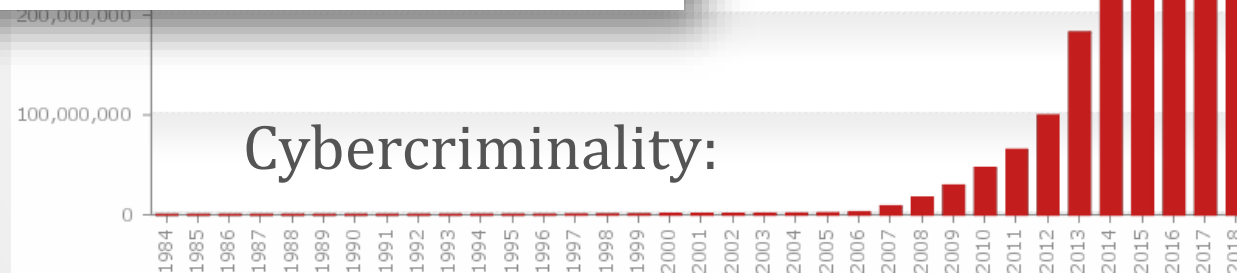
Hilton Hotels fined for credit card data breaches

🕒 1 November 2017



Hilton owns, manages or franchises 4,900 properties across the world

The company behind Hilton Hotels is paying a \$700,000 (£525,000) fine after being accused of mishandling two separate credit card data breaches.



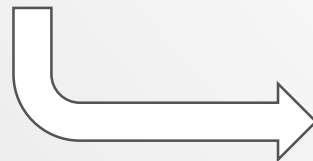
Last update: 02-01-2018 11:52

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

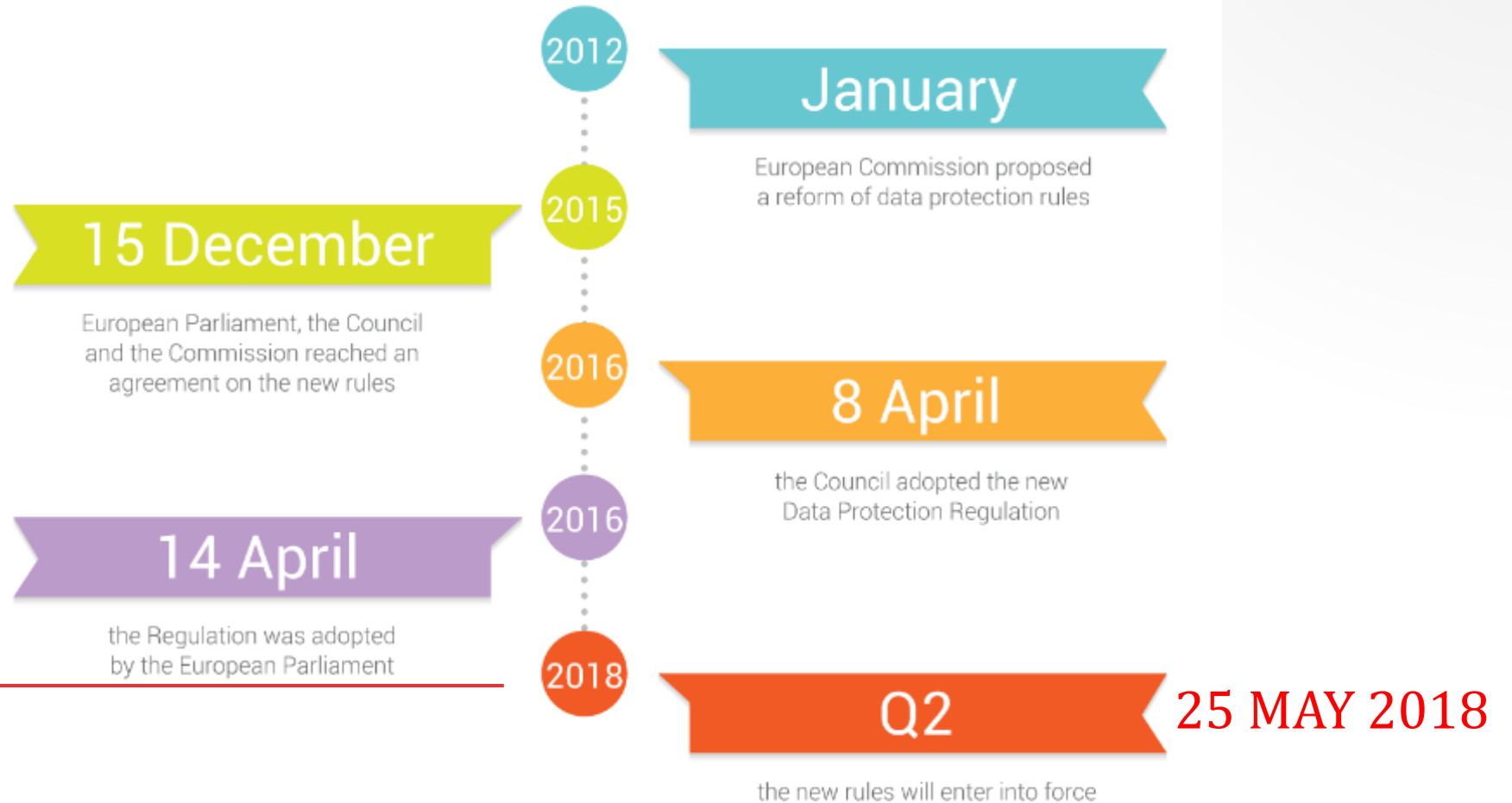


NEW DIRECTIVE

TIMELINE



Today : 28 different interpretations of the Directive of 1995



TERRITORIAL SCOPE



Established in the EU / Concerning EU citizens
Applies **worldwide** to whoever sells goods or services to EU citizens



PERSONAL DATA



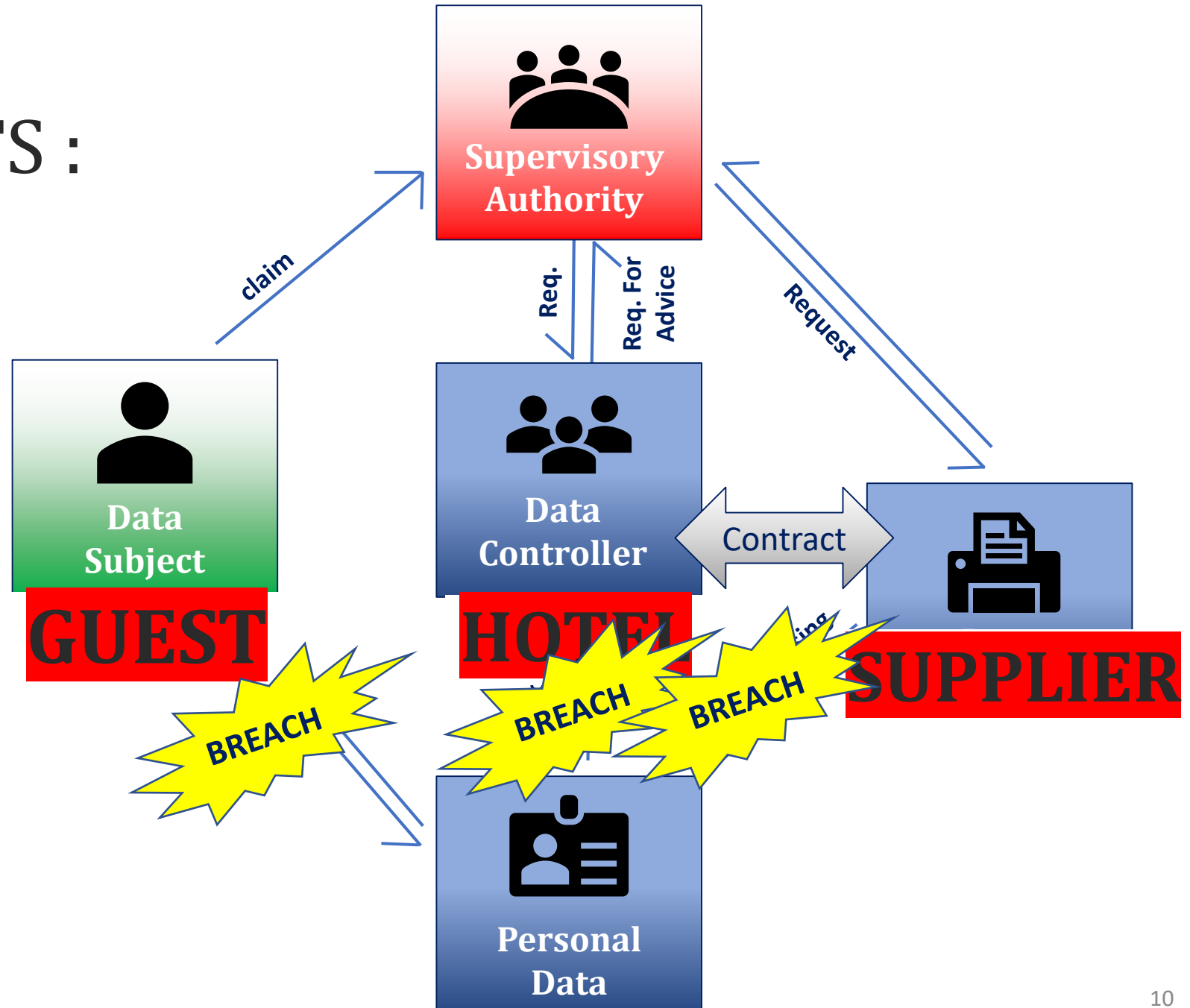
EXE

Name	Y
Birthdate	Y
IP address	Y
Blood type	N
Sexual orientation	Y
Biometric data	Y
Email address	Y
Bank account	Y
Room number	N
Food allergies	Y sensitive
Union membership	Y sensitive
Zip code	N
Company VAT number	N
Picture of a person	Y

>< **Natural person**



KEY CONCEPTS :



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
	PMS	27/03/2014	
	RegCard	01/01/2018	01/03/2018

Ideally automated ...



EXERCISE HOTEL-ROOM

EXE

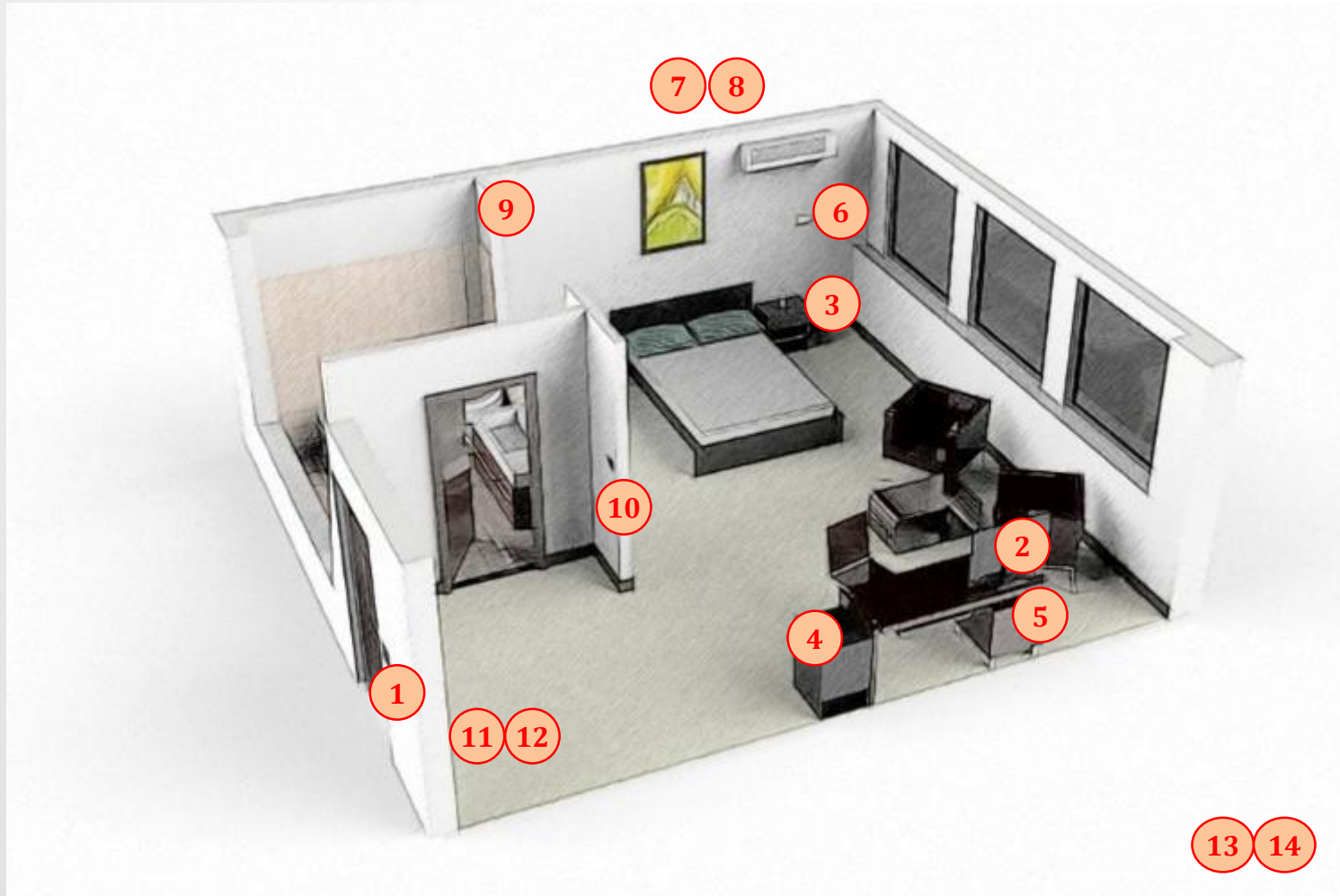


- Identify all possible systems
- Which ones process **PERSONAL DATA**



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

1

CREATE AWARENESS

2

CREATE GDPR REGISTERS

3

COMMUNICATE TO YOUR CUSTOMERS

4

RISK ANALYSIS

5

PROCEDURES





CREATE AWARENESS

Deliverables	
Inform entire hotel team	Awareness session PPT

A lot of information exists
Presentations exist :

Commission de la vie privée

Privacy commission

Commissie bescherming persoonlijke levenssfeer

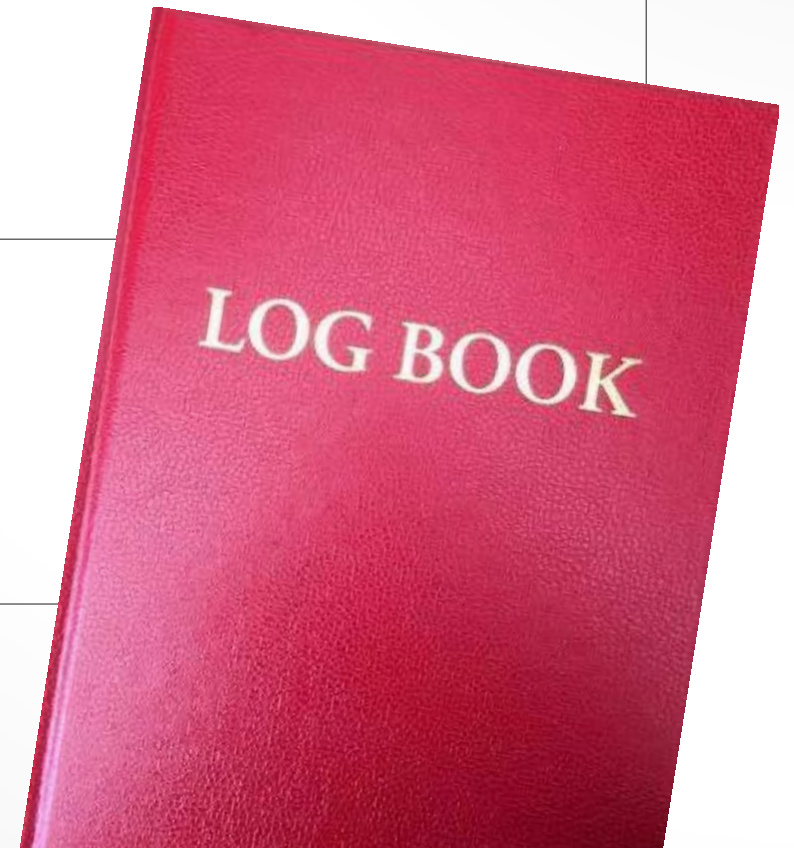
www.privacycommission.be



2

CREATE 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
<ul style="list-style-type: none"> • GDPR Logbook • Register of processing activities - Processes • Contracts Register • Risk Register 	
<p>In future</p> <p>Will also include</p> <ul style="list-style-type: none"> • Guest requests • Breach notifications 	



EXAMPLE “GDPR LOGBOOK”

EXE

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

(mandatory)

- 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

(mandatory)

EXE

IN GROUP :

- Identify as many processes – which process personal data - as possible “in your sector”
- Use flip-chart

00:15'



REGISTER OF PROCESSING ACTIVITIES

(mandatory)

- 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	





COMMUNICATE TO YOUR CUSTOMERS

Deliverables	
Create / Amend existing Privacy Policy	WEB
Are all rights of the customer mentioned ?	
How can the guest 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



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

RISK 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 hotel 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	RISK SCORE		
	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

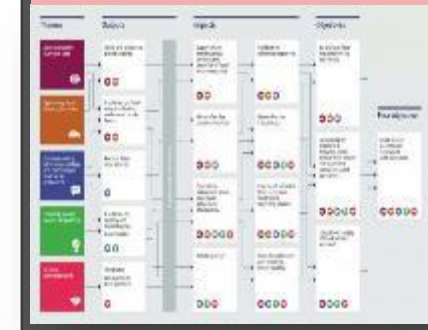
COMMUNICATE TO YOUR CUSTOMERS

4

RISK ANALYSIS



ACTION PLAN



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



1

CREATE AWARENESS

2

CREATE GDPR REGISTERS

3

COMMUNICATE TO YOUR CUSTOMERS

4

RISK ANALYSIS

5

PROCEDURES





PENALTIES

Fines of **up to 20 million €** or **4% of annual global turnover**, whichever is the greatest

Turnover is total SALES (GROUP)

Example

100 million €

4%

4 million €





kris@qhotelservices.com
www.qhotelservices.com