General Data Protection Regulation
AGENDA

• 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
EXPLOSION OF DATA

GPS
Google
Amazon
Facebook
Apple
Nearly Half of the Norway Population Exposed in 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

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
EXPLOSION OF DATA BREACHES

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.

Cybercriminality:
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

15 December
European Parliament, the Council and the Commission reached an agreement on the new rules

14 April
the Regulation was adopted by the European Parliament

2012
January
European Commission proposed a reform of data protection rules

2015

2016
8 April
the Council adopted the new Data Protection Regulation

2016

2018
Q2
the new rules will enter into force

25 MAY 2018
Established in the EU / Concerning EU citizens
Applies **worldwide** to whoever sells goods or services to EU citizens
## PERSONAL DATA

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Y</td>
</tr>
<tr>
<td>Birthdate</td>
<td>Y</td>
</tr>
<tr>
<td>IP address</td>
<td>Y</td>
</tr>
<tr>
<td>Blood type</td>
<td>N</td>
</tr>
<tr>
<td>Sexual orientation</td>
<td>Y</td>
</tr>
<tr>
<td>Biometric data</td>
<td>Y</td>
</tr>
<tr>
<td>Email address</td>
<td>Y</td>
</tr>
<tr>
<td>Bank account</td>
<td>Y</td>
</tr>
<tr>
<td>Room number</td>
<td>N</td>
</tr>
<tr>
<td>Food allergies</td>
<td>Y sensitive</td>
</tr>
<tr>
<td>Union membership</td>
<td>Y sensitive</td>
</tr>
<tr>
<td>Zip code</td>
<td>N</td>
</tr>
<tr>
<td>Company VAT number</td>
<td>N</td>
</tr>
<tr>
<td>Picture of a person</td>
<td>Y</td>
</tr>
</tbody>
</table>

>> **Natural person**
KEY CONCEPTS:

Supervisory Authority

Data Controller

Data Processor

Personal Data

GUEST

HOTEL

SUPPLIER

Claim

Req.

Req. For Advice

Request

Contract

BREACH

BREACH
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

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

Examples:
- 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
He makes the reservation himself (time of reservation)

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

<table>
<thead>
<tr>
<th>Consent Given</th>
<th>How</th>
<th>Date Given</th>
<th>Date Withdrawn</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>PMS</td>
<td>27/03/2014</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>RegCard</td>
<td>01/01/2018</td>
<td>01/03/2018</td>
</tr>
</tbody>
</table>

 Ideally automated ...
EXERCISE HOTEL-ROOM

- 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
CREATE AWARENESS
CREATE GDPR REGISTERS
COMMUNICATE TO YOUR CUSTOMERS
RISK ANALYSIS
PROCEDURES
A lot of information exists
Presentations exist:

Commission de la vie privée
Privacy commission
Commissie bescherming persoonlijke levenssfeer

www.privacycommission.be
## CREATE GDPR REGISTERS

<table>
<thead>
<tr>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>This LOG (« Bible ») should contain all steps taken by the hotel during the preparations and on-going phases leading up to May 2018</td>
</tr>
<tr>
<td>Register</td>
</tr>
<tr>
<td>• GDPR Logbook</td>
</tr>
<tr>
<td>• Register of processing activities - Processes</td>
</tr>
<tr>
<td>• Contracts Register</td>
</tr>
<tr>
<td>• Risk Register</td>
</tr>
</tbody>
</table>

In future

Will also include

• Guest requests
• Breach notifications
## EXAMPLE “GDPR LOGBOOK”

<table>
<thead>
<tr>
<th>DATE</th>
<th>WHAT</th>
<th>EXPLANATION - DECISION</th>
<th>REF</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 03 2018</td>
<td>Introduction to GDPR</td>
<td>Session d’info par VisitBrussels</td>
<td>visit.brussels</td>
</tr>
<tr>
<td></td>
<td>Start of Logbook</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plan d’action</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>....</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

IN GROUP:

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

• Use flip-chart
REGISTER OF PROCESSING ACTIVITIES

(mandatory)

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

<table>
<thead>
<tr>
<th>Create / Amend existing Privacy Policy</th>
<th>WEB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are all rights of the customer mentioned?</td>
<td></td>
</tr>
</tbody>
</table>
| How can the guest request access: | 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?
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 ....

<table>
<thead>
<tr>
<th>Data Risk</th>
<th>Probability</th>
<th>Impact</th>
<th>Technology Risk</th>
<th>Probability T</th>
<th>Impact T</th>
<th>RISK SCORE</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

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
## 5 PROCEDURES

<table>
<thead>
<tr>
<th>Deliverables</th>
</tr>
</thead>
</table>
| Guest Requests:  
• 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) | 100 million € |
| Example | 4% |
|  | 4 million € |