Road to GDPR compliance from the hospitality business perspective

2019

ACCOR

ACCOR

Live Limitless

Hotel Network

4,800 Hotels

704,000
Rooms

100 Countries

Hotel Portfolio

50 Brands

of which

38 Hospitality
Brands from Luxury
to Economy

To welcome our guests

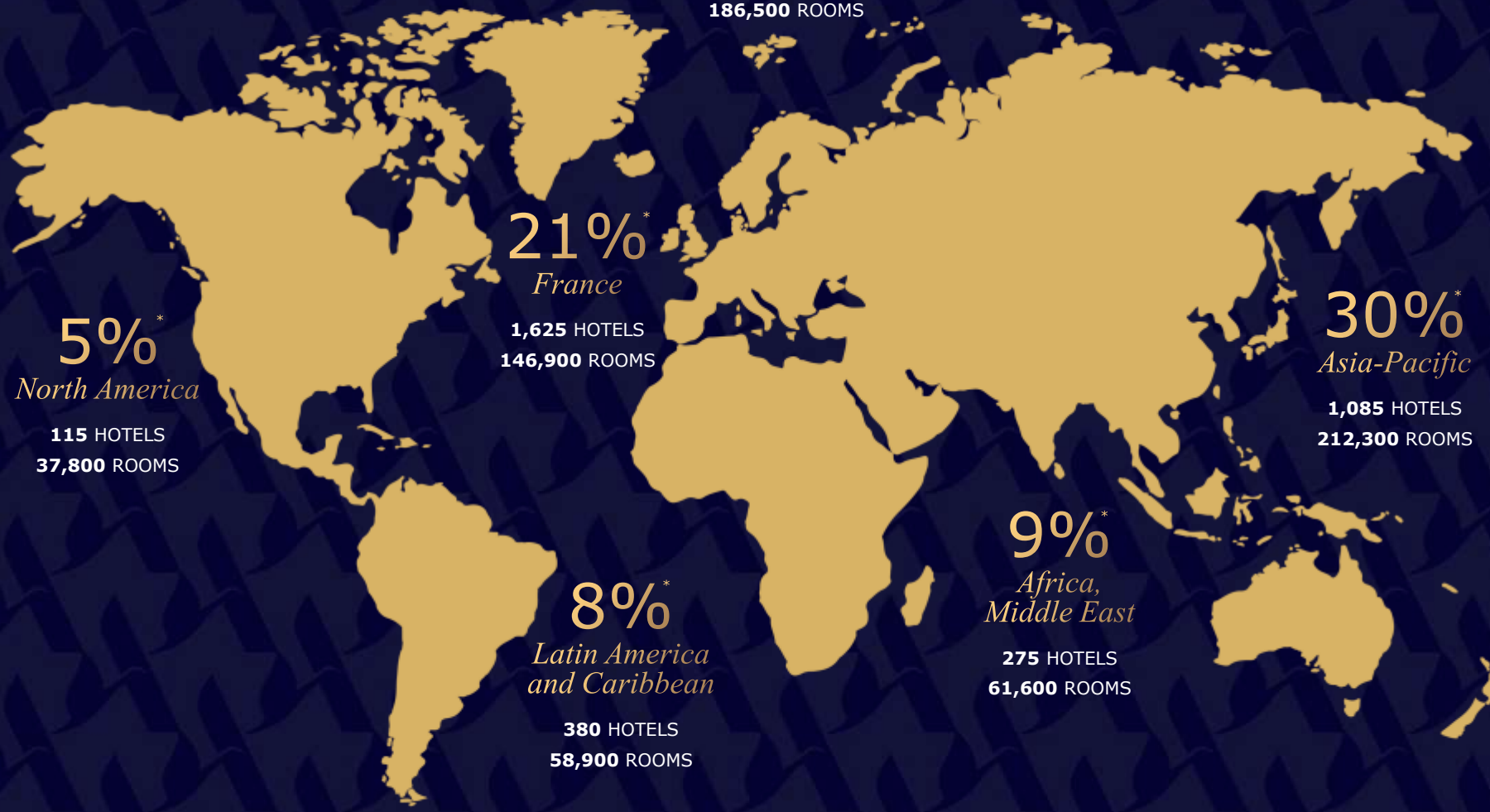
280,000
Employees
in Accor Brands

Pullman Bangkok Grande Sukhumvit - Thaïland

Accor, a worldwide hotel operator

4,800 hotels
704,000 rooms
100 countries

1 hotel opened every 29 hours



27%* *Europe*
1,320 HOTELS
186,500 ROOMS

21%* *France*
1,625 HOTELS
146,900 ROOMS

5%* *North America*
115 HOTELS
37,800 ROOMS

30%* *Asia-Pacific*
1,085 HOTELS
212,300 ROOMS

9%* *Africa, Middle East*
275 HOTELS
61,600 ROOMS

8%* *Latin America and Caribbean*
380 HOTELS
58,900 ROOMS

ACCOR
Live Limitless

* As a percentage of total number of rooms of Accor managed and franchised hotels, as of December 31, 2018.

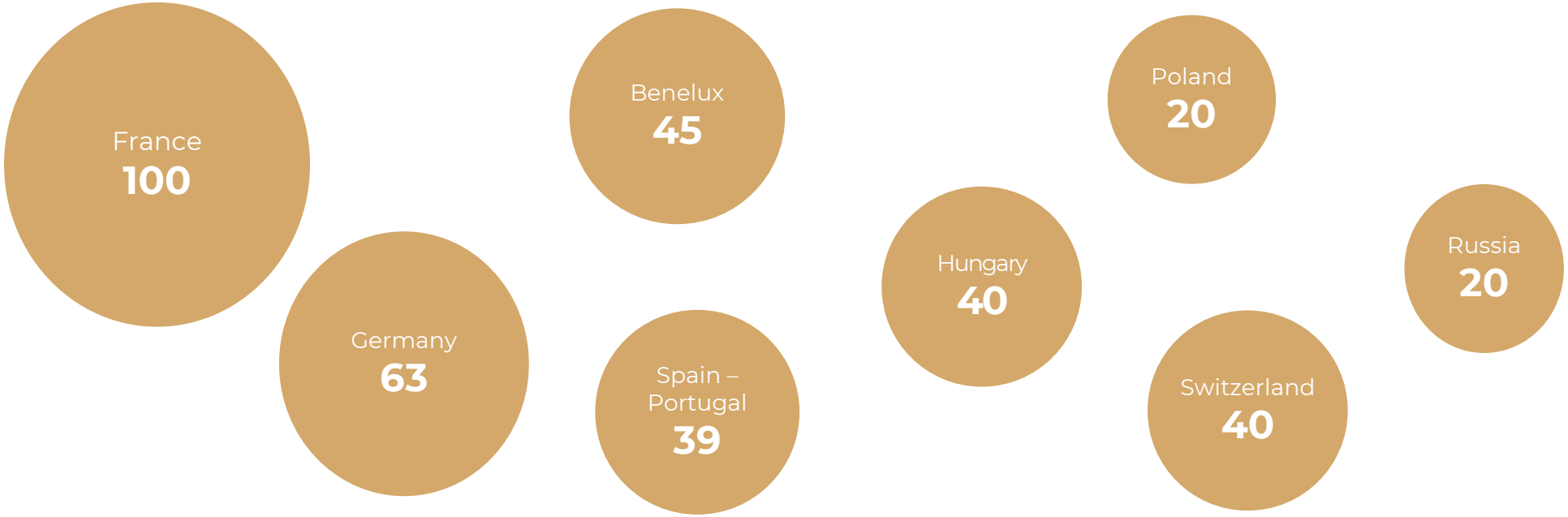
Number of identified personal data processing activities

BY COUNTRIES

Very wide spread of the number of personal data processing from one country to another.

It may suggest differences in the identification methodology (purpose grid, approach…), considering that data processing activities should not significantly vary for Business Units with similar business processes.

- Understand how each country has scanned and identified potential data processing to ensure consistency



Change of philosophy in approach to personal data

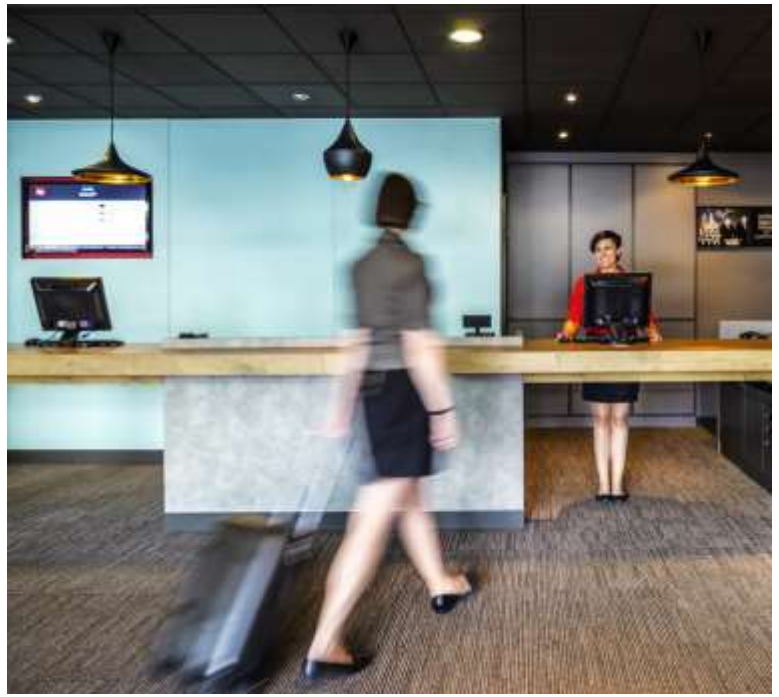
INTERDISCIPLINARY APPROACH

- Modified approach to the state of „compliance” - constant and open process instead of predefined list of compliance requirements
- Building-up the data protection awareness - “dispersed” risk control model that requires constant engagement of different business stakeholders,
- Interdisciplinary approach – policies supported by e-learning toolkit and internal trainings.

Features of personal data protection activities

PURSUED IN ACCOR GROUP

- Data mapping: „local" and „central" data processing activities,
- International loyalty programs,
- Personalization of the guest stay,
- Disclosure of personal data for the benefit of the external business owners (Accor's franchised and managed partners),
- Cross-border data flow, including data processing outside EEA.



Main encountered legal challenges

DATA PROCESSING

- Consistency of GDPR compliance among business units operation in different legal cultures and jurisdictions,
- Provision of privacy notice (organized groups and phone reservations),
- Data mapping - identification of personal data processing activities and flow of personal data within AccorHotels Group,
- Necessary to determine entities position related to data processing, identify processors and conclude intra-company data protection agreements,
- Handling of the data subject requests.

Main implementation phases and deliverables

IMPLEMENTATION PROCESS

Mapping of personal data activities

Records of processing activities (RPA) covering in particular:

- Description of processing activities
- Data retention periods
- Proposed purposes and legal bases
- Relationships between entities captured in RPA

Gap analysis and definition of recommendations

GDPR compliance gap report including:

- Brief summary of compliance with GDPR
- Recommendations for implementations and prioritizing of remediation measures
- Suggestions for improvement of the security measures

Implementation of outstanding measures

Provision of internal templates, procedures and guidelines

- Update of RPA (after implementation)
- Performance of DPIA (data Processing Impact Assessment) or LIA (Legitimate Interest Assessment)
- Adoption of IT toolkits to facilitate the governance

European project of data mapping process

MAIN STAGES

Context of creation of the GDPR Data processing register project:

- All Accor Group European regions had to map, document and analyze all personal data processing activities.
- The objective was to constitute the processing register according to GDPR requirement and to identify compliance remediation actions for each data processing.

Main stages of this approach:

1) **Conducting of GDPR interviews and workshops** to asses the activities and build-up personal data awareness,
2) **Build-up of AccorHotels Governance –** identification and overview of the business stakeholders,
3) **GDPR data processing register –** performance of personal data activity assessment (mapping, documentation, risk assessment and gap analysis),
4) **Introduction of the approved assessments into the GDPR toolkit.**

Layer's of GDPR implementation

3 LEVELS

GDPR compliance within Accor Group entities is handled at 3 levels:

1st level Accor SA	2nd level Orbis SA	3rd level Affiliated companies/ hotel
• GDPR compliance of centrally used applications/policies • Maintenance of central databases	• GDPR implementation coordination • IT security issues • Templates and training materials	• Handling data subjects requests • Managing of „local" databases • Ongoing compliance

Approach to the business owners

IMPLEMENTATION PROCESS

- Business owners – separate companies that operates their business under one of AccorHotels brands (franchised or managed hotels) – shared reputational and brand risks,
- Deployment of data mapping IT toolkit among the business owners,
- **Three layers of the data flow:**

Owner

Data controller with respect to:

- Guests data contained in the hotel's databases
- Hotel's employees data
- Service providers data
- Corporate clients data

Manager

Data controller with respect to: Manager's employees employed in the hotel

Data processor with respect to Services provided for the benefit of the owners: IT, procurement, marketing.

Accor Group

Data controller with regard to:

a) Accor (central) guest databases – central reservation systems
b) Group loyalty program.

Joint data controller
Group level personalization program deployed on the basis of joint data controllership agreement.

Personalization of the stay

DATA PROCESSING

- Main purpose: provide personalized, high quality service
- IT toolkit implemented to collect personal data from the guest deployed among Accor partners and business units,
- Vast amount of guest data with restriction to collect sensitive data,
- Joint data controllers relationship,
- Legitimate interest as the adopted legal basis for data processing.

Identified GDPR gaps

- Provision of privacy notice to the members of organized groups,
- Discrepancies related to manner of consent obtaining (consent collected over the phone),
- Discrepancies related to purposes covered by the consent - two different purposes for processing covered by one consent (receipt of commercial communication and membership in the loyalty program),
- Absence of dedicated person as internal coordinator responsible for agenda related to personal data,
- Collection of „excessive" data – collection of scan of credit/debit card in order to pre-authorize a payment.

Data subject requests

- Dedicated central privacy team to deal with requests submitted by the guests
- Adoption of one-stop mechanism (CNIL acting as the leading supervisory authority for Accor Group)
- Implementation of the data request handling manual. Main aims covered by the document:

1. Determine who, as the data controller, is authorized to handle the request (Accor S.A. or local business unit);
2. Be precisely informed of the type and scope of the request;
3. Verify the identity of the person who makes the request.

Data breach incidents

RISK ASSESMENT

- The crucial from Supervisory Authority perspective is to implement the data breach incident policy including the risk assement methodology.
- Factors taken into consideration to asses the risk:

a) Categories of personal data,

b) Amount of data,

c) Categories of data recipients,

d) Place of data processing,

e) Subcontractors involved in data processing,

f) Application of new technologies.

Data breach incidents

EXAMPLES

- Usually we are dealing with daily and operational incidents. Examples of encountered incidents:

a) Capturing photo of the breakfast in-house guests list,

b) Disclosure of the guest data from the hotel's property management system,

c) Mistakenly dispatch of the emails to corporate client,

d) Erasure of document files including data without its proper disposal.

RAFFLES \ ORIENT EXPRESS \ BANYAN TREE \ DELANO \ SOFITEL LEGEND \ FAIRMONT \ SLS \ SO \ SOFITEL \ THE HOUSE OF ORIGINALS
RIXOS \ ONEFINESTAY \ MANTIS \ MGALLERY \ 21C \ ART SERIES \ MONDRIAN \ PULLMAN \ SWISSÔTEL \ ANGSANA
25HOURS \ HYDE \ MÖVENPICK \ GRAND MERCURE \ PEPPERS \ THE SEBEL \ MANTRA \ NOVOTEL \ MERCURE \ ADAGIO
MAMA SHELTER \ TRIBE \ BREAKFREE \ IBIS \ IBIS STYLES \ IBIS BUDGET \ JO&JOE \ HOTELF1