**Summary from GDPR's Impact on Travel Industry"**

Applies to all countries that process data of Europeans. So not JUST European hotels/companies. Especially in Travel this means that any hotel that accepts EU travellers needs to comply.

**Core GDPR Rights and Consequences**

**1.** Rights of access: everyone guest/person with personal data in your system has the right to know:

what the data is

where it is located

purpose of the data

how its stored.

**2.** Right to rectify/erase: The person should have the ability to delete the information. Note that this right may be refused, if you have a future booking coming up where the data is still required. Also if another law in the country states that the data needs to be stored after the departure, than that law supersedes the GDPR.

**3.** Data Portability: It should be possible to export personal data (in a widely accepted format), in case a customer would want to move to another platform (designed if for example someone wants to leave Facebook, and migrate to another platform... but even though this is the specific use case it was built for, its not exclusive to this use case.

**4.** Profiling & Right to Object: If a system analyses the guest profile, and changes the customer experience based on what was learned from the profile, then the customer may request to know about this process. For example if specific types of people get a special deal, based on their profile (for example Oaky, who offers different things to business and leisure guests). If we use profiling as part of our business application, then it has to state this explicitly in the contracts (Mews: I assume in the Data Privacy Policy)

Audience Questions

What is personal data?

Anything that can be used to identify an individual (name, phone, cc number, IP address, etc).

Does the GDPR apply retroactively?

Yes, it applies to all data. So if its old data, you need to either delete it, or ensure it complies.

Who is liable for the data compliance

Everybody in the process are completely liable. If you can proof that you have done everything needed to comply, then the blame shifts to the other party. The burden of proof is on everybody involved in the transaction.

Obligations

**1.** Data Protection Officer (DPO)

- Somewhat independent, yet still capable of implementing policies in that company at exec level. His role is to advocate the customer’s privacy

- Cannot report to CMO or CTO, so needs to sit in a separate hierarchy.

- You can hire an outside person to do this (ie. lawyer)

**2.** Data Protection Impact Assessment (DPIA)

How will new changed/project impact customer privacy. So the DPO has to be involved in designing all new workflows/processes

**3.** Breach Notification:

Nobody is allowed to keep a hack under wraps. If you have any belief that there was a breach, this needs to be reported to a local officer in the member state. Then in turn the controller needs to contact the customer with information about the breach. The officer needs to be informed within 72 hours of finding out about the breach.

**4.** Lawful Basis and Types of Consent:

Explicit Consent (similar to cookie consent on websites): some aspects would require this.

Travel Specific Implications

**1.** Profiling for revenue optimisation purposes. For example loyalty, IP address, previous spend. If you are using this data to create a custom offer, then this needs to be clearly shown to the customer. For example Oaky/Nor1: customer has the right to see how the discounted price they are offered for an upsell is compiled

**2.** Cross-border implications of transactions. If we are the data controller, and there is a breach a customer just sue Mews. So if we work with a company that does not comply with GDPR, we may become liable on their behalf… as we made the decision to work with that company

Discussion points for MEWS

- What data can we simply delete from our system? There is no need to extra data that you do not need

- Pick one country, where we will have a representative who is in contact with the authority of that country (what language will we use?)

- Tools: compliancy support framework - there are many companies in this space… investigate

- Hire someone to penetrate our own security systems

- 72hours deadline: "Incident Management Tools” to compile info quickly, and who to notify, etc.

- Forensic Tools, to systematically analyse why and how the breach happened.

- Appoint DPO asap

- Review the backoffice solutions that Mews is using to process personal data (pipe drive, etc)