A Hotel's GDPR journey

techtalk.travel

Discover → Manage → Protect → Report

1 DOES YOUR HOTEL KEEP TRANSPARENT RECORDS DEFINING...

- Purpose of processing.
- Categories of personal data processed.
- Identities of third parties with whom data is shared.
- Third countries that receive data & the legal basis of such transfers.
- Organisational & technical measures being implemented for compliance.
- Data retention purposes & time limits.

No: *Using Auditing tools ensure processing of data (collection, sue, sharing etc) is tracked & recorded.*

Yes: *GDPR's global standards in data transparency, accountability & record keeping.*

01 Hotel Technology vendors who processes guests' personal information for any purpose.

2 DO YOU HAVE A BREACH NOTIFICATION PLAN?

No: *Set clear expectations built into your contracts for potential breach notifications.*

Yes: *Set clear expectations built into your contracts for potential breach notifications.*

02 Required Technologies
- Monitoring.
- Protecting.
- Reporting and Analytics.
- Auditing.

Article 32: The hotel shall without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

3 DO YOU HAVE A DATA GOVERNANCE PLAN FOR HANDLING DATA SUBJECT REQUESTS?

No: *Implement the Incident Response Management Process.*

Yes:

Section 2: Information and Access to Data.

Section 3: Rectification and Erasure.

Section 4: Right to Object and Automated Individual Decision Making.

03 Examples of GDPR Software tools that can be used:
- NAVEX Global.
- LogicGate.
- ZenGRC.

4 HAVE YOU COMPLETED A DATA PROTECTION COMPLIANCE REVIEW?

No: *Hotels must have their DPO conduct DPIA's and reviews that are continuous with reports on any compliance gaps that your hotel must address and report to the Supervisory Authority.*

Yes:

Article 35: The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Conduct a Data Protection Impact Assessment (DPIA) to assess the state of your hotels level of Data Protection.

TRAIN YOUR STAFF

12 STEPS OF GDPR COMPLIANCE

1. **Awareness -** All employee engagement, creating a culture of opportunity & respect for data.
2. **Information you hold -** Mapping what personal data you capture, where it is captured & who has access.
3. **Communication -** Ensure your privacy statements are clear and fit for purpose.
4. **Individual Rights -** Understanding individuals rights, including Data Portability and Right to be Forgotten.
5. **Subject Access Rights -** Evaluating current procedures and ensuring you can provide information within new timeframes.
6. **Legal Basis for Processing Personal Data -** Evaluating your legal standpoint for capturing personal data & ensuring compliance with new restrictions.
7. **Consent -** Evaluating how you are collecting and recording consent, ensuring it is compliant & evidenced.
8. **Consider Children -** Considering how you will verify individuals ages and/or parent consent.
9. **Data Breaches -** Ensure you have a process in place to inform the European Data Protection Supervisor (EDPS) in the EU and if in the UK, it's the ICO (Information Commissioner's Office).
10. **Data Protection by Design/Data Protection Impact Assessments -** Considering how GDPR affects your business and how and when you need a Data Protection Impact Statement.
11. **Data Protection Officer -** Ensure you have a member of staff responsible for your hotels compliance with Data Protection.
12. **Think Internationally -** If your hotels operate in more than one EU member state (i.e.cross-border processing), you need to determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

3rd Party Data Processing Checklist

Hotels need to check the following items without fail for any technology provider processing guest or staff personal information for any purpose.

- Determine the type of data the vendor processes.
- Determine the purpose for which the processing is happening.
- Obtain a Data Processing Agreement.
- They, together with the appropriate agencies / bodies that provide companies both in the country from where the vendor is from, and in the EU with a mechanism to comply with data protection requirements when transferring personal data from the European Union to that country. Ensuring there is a lawful basis for transferring the data.
- Mention the vendor in the hotel's privacy policy, along with the purpose of the vendor and how the data will be used.
- Confirm that the vendor can handle data rights requests with a SLA under 30 days.

GDPR Compliance 8 Point checklist.

GDPR compliance is not a journey with a clear ending.

Continuously assess your data inventories & practices to ensure your company is up-to-date with protection regulations.

01 Awareness & Communication

02 Analysis of Personal Data

03 Review Procedure

04 Access Rights

05 Customer Consent

06 Data Breaches

07 Impact Assessments

08 Data Protection Officers - DPO

NEXT STEP

GO BACK TO STEP 1 TO MAKE SURE YOUR INFORMATION IS PROPERLY CLASSIFIED.

techtalk.travel