HFTP®
Hospitality Financial and Technology Professionals

EU General Data Protection Regulation (GDPR)

Compliance Tools for the Hospitality Industry

LETTER TEMPLATE:
Vendor Compliance Query

The attached letter is a template intended to be used by lodging organizations to inquire about GDPR compliance from their vendors. The letter asks vendors to submit their current data security and privacy practices and to describe the steps they are taking to become compliant ahead of the GDPR deadline of 25 May 2018. The letter is meant to act as a starting point, to be customized for an individual organization.

This template was developed by the HFTP Hospitality DPO/GDPR Task Force. The task force is a group of 23 hospitality industry experts tasked with developing hospitality-specific guidelines to assist with preparation for GDPR compliance.

The General Data Protection Regulation (GDPR)

Letter Template: Vendor Compliance for a Company

[Recipient],

The legislation of the European Union's General Data Protection Regulation (GDPR) and its deadline of 25 May 2018 for compliance is just on the horizon — and so this is an opportunity to assess our digital eco-system, both in terms of networks, as well as operations.

We therefore need to review our vendor contracts as:

1. We intend for our guests to continue to be confident that while lodging with us, that their persons as well as their personal information will be secure.
2. Our reputation will rely upon our use of your systems.

As our partner, we ask that you join us in the assessment of data security and privacy measures, from the technical to the procedural.

We need to evaluate the data security protocols of your product(s) and service(s) as well as to understand your company's commitment and vision via your statement of GDPR compliance for the product(s) and service(s) that you provide to us.

This is required as we believe that GDPR compliance will be 'business critical' for any business providing goods or services to EU (European) residents from May 2018. This applies to any personal information held on our guests and where it is stored — which may well affect our business contract in terms of where our guest information records are stored (in the cloud).

It is very unlikely that any contract we have will have anticipated the GDPR requirements and, so we require an initial response from you that confirms:

A) Your company's general statement and policy on the products becoming GDPR compliant

B) A timetable for the above (pre-May 2018)

C) Confirmation of where our data is stored (if applicable)

D) A timetable for agreeing to any legal contract changes to take GDPR compliance into effect

Please confirm at least receipt of this letter as soon as possible.

Any failure to respond by 31 December 2017 will suggest to us that your product(s) or service(s) to us are not likely to be GDPR compliant and we will, therefore, have to review an alternate supplier to avoid any potential fines that may be foreseen within the regulation.

GDPR is all about the guest's right to privacy for their data. We are aiming for certainty that our data strategy at least achieves the obligations of maintaining compliance to the GDPR. It is the least we can do for our guests.

Kind Regards,
[sender]