The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) will become law within the European Union with effect from 18 May 2018.
The Data Protection Commissioner, has stated the following on their website:
"GDPR very significantly increases the obligations and responsibilities for organisations and businesses in how they collect, use and protect personal data. At the centre of the new law is the requirement for organisations and businesses to be fully transparent about how they are using and safeguarding personal data, and to be able to demonstrate accountability for their data processing activities."
The implementation of GDPR addresses the storage of customer data. Our position at In1 has always been, that you should only store information that is relevant and only retain it for as long as it is useful. This also improves your bottom line as less form filling at the booking / purchase stage improves the conversion rate. And it also reduces your obligations under GDPR, remember GDPR is about personally identifiable data.
There is no longer a need, for example, to retain the postal addresses of a customer. Why bother, no one uses the postal services to communicate and holding this data for no purpose simply increases the obligation to protect such data. In fact, keeping data for no good reason or where there is no process for using such data breaches GDPR as you are only to keep data that you require to service a transaction. Similarly, with phone numbers, do you really need them after the guest has departed, maybe for a short time in case something is left behind in the room but do you really need a guest phone number 30 days after departure. If you are never going to call, then don't keep it. Less is better.
Credit/Charge card data has long been subject to stringent controls. All In1 technologies both partner and guest facing, are SSL Secured and PCI DSS Compliant. We never store or supply Credit Card CVV's as this is in breach of your Credit Card Merchant agreement and entails serious fines. The moment a transaction is complete we obfuscate Credit Card information. Where servers and services comply with PCI/DSS they must comply with a level of security of access meeting with best technical practice, a significant part of the obligation under GDPR. When you have customer data, keep it safe and secure.
GDPR implemented correctly can enhance your business and should be approached in that spirit.

- Build customer trust
- Improve brand image and reputation
- Improve data governance
- Improve information security
- Improve competitive advantage

Although there has been a certain degree of scare mongering to date, the objective of GDPR is to advise and improve data security. Those that consciously and deliberately abuse the data security of their customers and fail to implement corrective actions, or cease their abuse once advised or warned, can rightly expect a degree of censure. Those who do not respect customer security and confidentiality endanger online commerce and customer trust and should rightly be brought to heel.
Those that work to comply with GDPR and follow guidance or advice to improve their processes should not expect to be punished or fined. This is what the Data Protection Commissioners across Europe have stated as their objective. They wish to advise, educate and improve data security, not penalise genuine businesses working toward GDPR compliance.

Data Storage – Customer Contact Details

In1 Solutions is very much aware of the obligations that its accommodation, catering and retail partners must adhere to when gathering, storing and using customer information. We have been consistently ahead of the evolving requirements for privacy and security in terms of the financial and personal data of the guest / purchaser.

We have long made available and recommended the short form version on your room or voucher booking engine payment form when collecting customer data. This limits the information to First Name, Last Name, Email Address, Phone Number, and Country of Residence.
We do not use customer data directly, it is not ours to use, but that of our hotel, catering and retail partners. We simply act to collect the minimum amount of information possible to support a transaction and pass that information on securely.

Credit Card Information

The In1 Solutions booking engine and voucher engine uses SSL certificates to ensure that all data transferred between the web browser and the web server is secure. This is visible to the booker via the green secure padlock in the address bar of the browser when guests are making a booking or purchasing a voucher.
The credit card details supplied during the booking process are obfuscated in accordance with PCI DSS compliance. We never store CVVs. All customer data is stored on secure servers that are PCI DSS compliant. We also store the software necessary to send email campaigns on these secure and compliant servers.

Customer Consent

The GDPR explains how an organisation should obtain customer consent in order to use customer email addresses for marketing purposes.
"They must know exactly what they are consenting to, and there can be no doubt that they are consenting. Obtaining consent requires a positive indication of agreement – it cannot be inferred from silence, pre-ticked boxes or inactivity".
To ensure compliance, In1 Solutions advises hotels to enable the positive opt in for email communication in the final stage (payment) of the booking and voucher engine. That positive opt in explicitly obtains the consent of the customer to use their email address for future marketing communications. This will enable hotels to prove that personal data was collected in compliance with GDPR and a record will be retained showing when, why and how the data was collected. It will also show that it was used in a manner that is compatible with the initial reason for collecting the data.
The options for short form and email opt in are available for configuration in the IMC. If you have any queries, please contact In1 Support.
Where your website is developed by In1 Solutions we are contact each website administrator regarding any data collection beyond the utilisation of the GDPR Compliant In1 Booking Engines. In the main this consists of newsletter opt in and contact form. Where you collect data, you must ensure that you have the positive confirmed knowledge and permission to collect, hold and utilise this data.
Where you have collected customer information prior to GDPR, we would advise you to minimise such information on a need to have basis. Should you no longer need to communicate with those customers then you should obfuscate or delete that data. Where you do communicate using such information you should always offer an unsubscribe.

Right to be forgotten

A basic tenet of GDPR, is the right to be forgotten. In1 will accept direction from its customers, clients and partners at any time to obfuscate or delete (forget) any information relating to an end user (collected via In1 Online Engines or Newsletter/Email opt-in) at the direction of the merchant (e.g. hotelier, restaurant, retailer, etc.). We commit to doing so within 14 working days of written (email will suffice) instruction.
Where we are approached directly by an end user, we will commit to exercising a forget, no later than 30 working days of receipt of written (email will suffice) instruction and will notify the merchant in the interim of the instruction received and our commitment to do so. We inform the merchant, to ensure there is no ongoing issues between merchant and guest where a delete, would cause a difficulty.