

How we use your information

This privacy notice tells you what to expect when ILG Business Limited (“ILG Business Limited, we or us”) collects personal information. It applies to information we collect about:

- visitors to our websites
- Individuals in relation to a data protection or freedom of information complaint or enquiry
- people who notify under the Data Protection Act

Privacy Statement

ILG Business Limited has created this privacy statement in order to demonstrate our firm commitment to privacy.

General Statement of Principles

As described in detail below, any information we gather at this web site is strictly for our use and is not shared with any other entity, public or private, for any reason. We will not sell or give away any lists or other data that we may retain.

Statistical Data

Our servers (as most) track IP addresses and referring pages to help with site maintenance and improvements. This data is viewed only as anonymous statistics to show the busiest times of the day or week, pages with errors and how effective our advertising has been. This information is not used for any other purpose.

Personal Information Collected - Order Forms

The information provided on your order form is only used to allow us to track consulting issues or refer to a previous order to help provide customer service and we do not share this information.

We do not store any type of credit card information

Information Correction or Removal

You may elect to correct, update or remove any information about you that may be in our records

by e-mailing us at appsupport@ilgbusiness.co.uk with your request.

Data Protection

ILG Business Limited (ILG) undertakes to strictly limit access to all data, to the staff necessary for the performance, management and monitoring of the Contract.

ILG undertakes to adopt appropriate technical and organisational security measures having regard to the risks inherent in the processing and to the nature of the personal data concerned in order to:

1. prevent any unauthorised person from having access to computer systems processing personal data, and especially:
2. unauthorised reading, copying, alteration or removal of storage media;

3. unauthorised using of data-processing systems by means of data transmission facilities;
4. ensure that authorised users of a data-processing system can access only the personal data to which their access right refers.