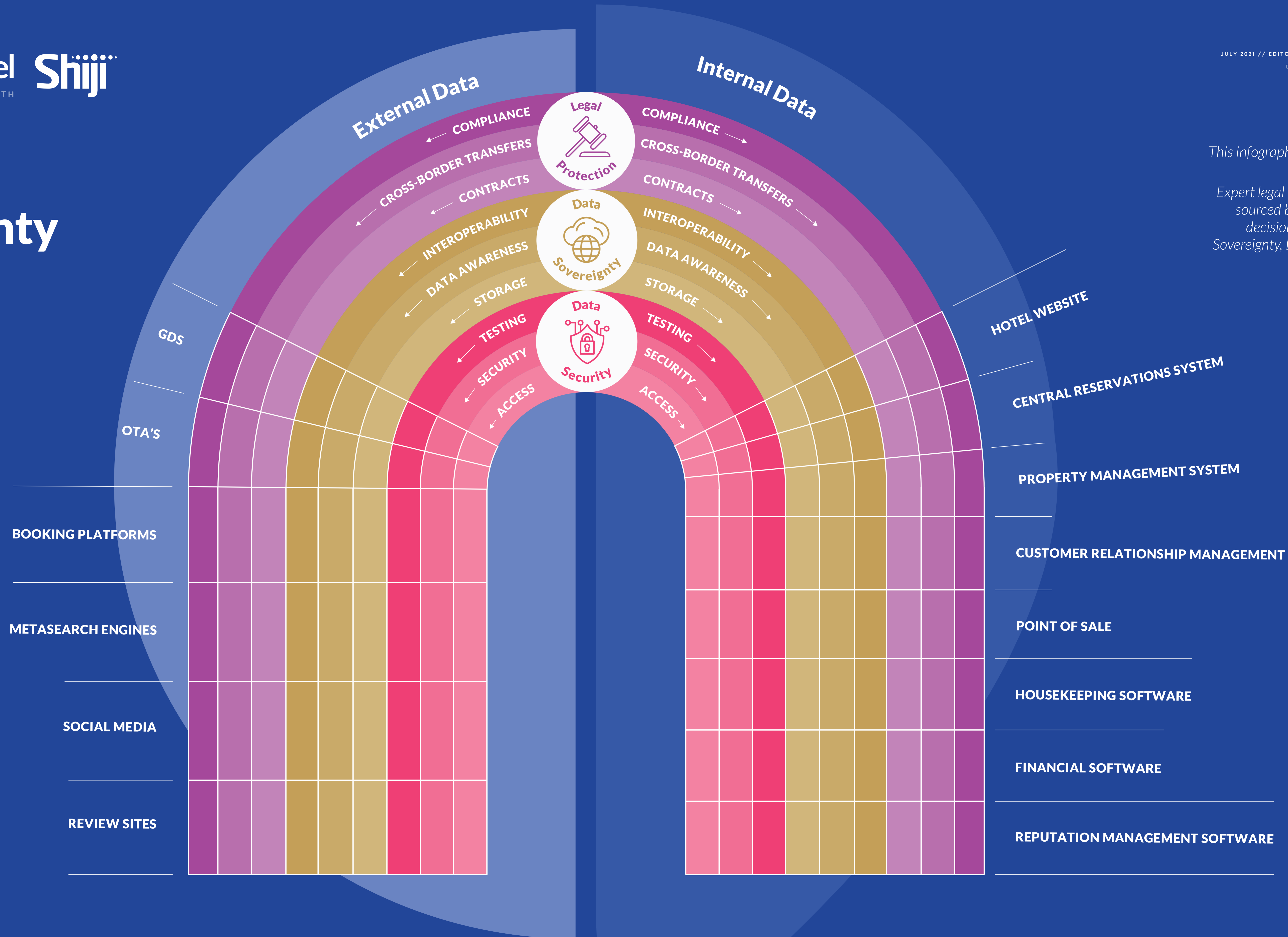


Data Sovereignty

Data sovereignty is the idea that data is subject to the laws and governance structures within the nation it is collected. The concept of data sovereignty is closely linked with data security and legal protection.



DISCLAIMER:

This infographic should be used purely as a guide. Expert legal counsel should be sourced before making any decisions related to Data Sovereignty, Data Security and Legal Protection.

Data Security

- ACCESS** Access is strictly controlled, logged and monitored.
- SECURITY** Backups, encryption at rest and in transit, storage location, pentesting, network security and access management.
- TESTING** Frequent penetration testing and up to date certification.

Data Sovereignty

- STORAGE** Company's must think where to store the data. Data is stored in Data Centers across the globe, either locally or internationally.
- DATA AWARENESS** Scope and type of data.
- INTEROPERABILITY** Connection of systems and services and data exchanged.

Legal Protection

- CONTRACTS** Executed Agreements defines the roles (Controller or Processor) and the obligations and liabilities of each party according to the type of data to be shared or stored between them.
- CROSS-BORDER TRANSFERS** Additional Agreements may be necessary, such as a Data Privacy Addendum or the newly revised Standard Contractual Clauses, and should be assessed regularly.
- COMPLIANCE** The global regulatory environment is evolving and requires continued evaluation to determine which regulations apply to a given situation and how (or if) your organization complies.