Regulatory and Security Overview:
JERSEY

Data Protection

The concept of data protection was introduced to the island in 1987 and the current regime is governed by the Data Protection (Jersey) Law 2005. In essence it is a form of consumer protection whereby an individual whose personal data is held by another can enquire about the data itself.

Most importantly, it does not give any third party rights to see that data - in fact quite the opposite. The owner of the data, "the data controller" (in this case our client) and the manager of the data "the data processor" (in this case Sure International) must adhere to a number of guiding principles and if anyone other than the data subject is allowed to see information, without an order by the Royal Court of Jersey, there would be a breach of the law.

Data Disclosure

A third party may seek to gain access to customer information but can only attempt to do so with such a Court Order. This might be in the course of an investigation into a criminal matter, for example anti-money laundering, or a civil matter, for example a matrimonial dispute. In either case, however, the Order would be served on Sure International and as a data processor the company is incapable of disclosing information that it cannot access. Information processed by Sure International is in an encrypted form (and is therefore not able to be viewed by us) and, even if inadvertently disclosed, it would be of no value to the third party as it would be indecipherable.

In the unlikely event that the customer itself sought access under the Data Protection Law, the response would be the same, because Sure International does not have access to the information.

Data Neutrality

Unlike some jurisdictions, Jersey does not have specific legislation requiring companies to store sensitive data within its territory; nor has it implemented the type of legislation that grants rights to the interception and seizure of data in the same way as the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) act or the RIPA (Regulations of Investigatory Powers Act) in the UK.

Jersey's law in this regard (RIPL – Regulations of Investigatory Powers Law, Jersey) is merely an extension of the traditional interception of communications legislation that has been modified to take account of developments in modern telecommunications. To be clear, no individual, body or government department has any statutory right of access to stored or transmitted data in Jersey. Access to this type of information can only be achieved through a court order that will only be granted by the Jersey Attorney General once he/she is satisfied that there is 'prima facie' evidence of a crime and recognised as such in Jersey.

The data requested must be relevant, proportionate and specific about individuals and time periods and therefore it is not possible to undertake so called 'fishing expeditions'. For these reasons Jersey is perceived to be a 'data neutral' jurisdiction for businesses from other countries and the extensive legal checks and balances that exist there make it a safe location where sensitive information cannot be inadvertently disclosed. This data neutrality is particularly attractive to organisations that wish to centralise a data depository for subsidiaries that might be in many different jurisdictions each of which have differing laws governing data.

sure. International
Batelco Group Member

Regulatory and Security Overview

External accreditation

Today, organisations can select from a variety of providers that claim to apply best practice in Information Security. However, how can you trust them? Do they apply best practice in technology security including process and procedures and how do they validate their claims?

Commitment to Governance and Information Security has to be driven from board level and is underpinned by an Information Security Management System (ISMS). In our case this has been independently certified by the British Standards Institute (BSI) to comply with the requirements of ISO/IEC 27001: 2005.

Its is important to understand that ISO 27001 is far broader than just IT: it interweaves the entire business function and its supporting back office processes. Certification is a major exercise and becomes the core component of a company's culture. If you trust your data to a third party, these standards should be the minimum benchmark.

Security

We regard the security of clients' data as being of paramount importance. Physical security is achieved by several means: three-stage secure access controls to the datacentre for identification, verification and perimeter security; 24x365 monitoring from a permanently manned Network Operations Centre (NOC); video footage from numerous strategically located cameras attached to long-term storage and proximity-card access reading software; and finally, all our equipment is monitored and managed from our 24x365 NOC.

Summary

The only entity able to disclose any stored information is the customer (the data controller) and thus any party seeking information would have to address that request, either under the Data Protection Law if a customer, or pursuant to a Court Order, directly to the data controller. The data protection environment in Jersey places an obligation on all Jersey businesses which hold personal data to comply with strict guidelines relating to the care of that data and prevent improper access. Combining this protective environment with the technical security measures we use means that the risk of disclosure is virtually nil and that the customer is most likely afforded greater protection in Jersey than in a jurisdiction without equivalent legislation.

sure. International
Batelco Group Member

Guernsey
Centenary House
La Vrangue
St Peter Port
Guernsey
GY1 2EY
01481 757757

Jersey
The Powerhouse
Queens Road
St Helier
Jersey
JE2 3AP
01534 888291

Isle of Man
2nd Floor
14 Athol Street
Douglas
Isle of Man
IM1 1JA
01624 692222

www.sure.com