BRIEFING NOTE

Regulatory & security overview

RELATING TO SURE INTERNATIONAL'S EMAIL SOLUTIONS

The Channel Islands (Jersey and Guernsey) policies on data protection and the security aspects of Sure International's Mimecast Offshore email solutions suite

Introduction - Data Protection & Disclosure

Sure International recognises that its clients operating in jurisdictions outside the European Economic Area may feel that they lack knowledge about the business and security implications of the Channel Islands legislation relating to data protection and disclosure.

This paper is intended to give some generic guidance for such organisations as well as a brief description of the Channel Islands relationships with the United Kingdom and the European Union. In addition, an outline of the security aspects of Sure International's Mimecast Offshore email solutions suite should go some way to explain the system's functions and processes involved in protecting your data.

eshore

Official Partner of:

sure. International

Regulatory & security overview

Sure International

Sure International has been offering datacentre and Internet services in the Channel Islands for many years, and is engaged in the provision of hosting, data storage and email services to ecommerce, legal and financial services companies internationally.

The Channel Islands

The Channel Islands are not part of the United Kingdom, but self-governing Crown Dependencies which gives the islands constitutional rights of self-government and judicial independence. These rights were granted by Royal Charter 800 years ago and are unaffected by changes to United Kingdom or European government.

This offers businesses and investors the benefits of an independent international finance centre, which is politically and economically stable and close to the United Kingdom and mainland Europe. The Channel Islands legislative assemblies, the States of Jersey and the States of Guernsey, have total responsibility for each island's domestic legislation, including taxation and financial regulation.

The Channel Islands have a special relationship with the European Union, defined by Protocol. Neither a member nor associate member, this relationship is ratified by Protocol 3 of the Treaty of Accession of the United Kingdom to the European Community. Through this Protocol, Jersey and Guernsey comply with European Union Directives on trade in industrial and agricultural products, but is not obliged to implement Directives or Regulations in other areas such as: European Monetary Union, Taxation and Financial Services.

Data Protection

The concept of data protection was introduced to the islands in the 1980s and the current regime is governed by the Data Protection (Jersey) Law 2005 and the Data Protection (Bailiwick of Guernsey) Law, 2001. 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 and Mimecast Offshore) 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 or Guernsey there would be a breach of the law.

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.

Security

Sure International regards the security of clients' data as being of paramount importance. We ensure the security of stored emails while keeping them online for clients' access 24 x 365. Physical security is achieved by several means: three-stage secure access controls to the datacentre for identification, verification and perimeter security; 24 x 365 monitoring from a permanently manned Network Operations Centre (NOC); video footage from numerous strategically located cameras attached to long-term media storage and proximity-card access reading software; and finally, all Sure International equipment is monitored and managed from our 24 x 365 NOC.

Technology

Security and client confidentiality are core parts of the Mimecast Offshore platform and all email content is automatically and uniquely encrypted within the platform. Neither Sure International nor Mimecast Offshore has access to view message content.

In general email data transits the Internet, largely in unsecured Simple Mail Transport Protocol (SMTP) sessions. Sure International and Mimecast Offshore address this lack of security by means of Transport Layer Security (TLS), which is used to negotiate a secure tunnel between a client's infrastructure and the Mimecast Offshore servers. The result is that all data travelling between Sure International and our clients' infrastructures is encrypted.

Regulatory & security overview

Secure communication between organisations is achieved by ensuring that both sender and recipient email infrastructures have a valid SSL (Secure Sockets Layer) certificate and then setting up a unidirectional or bidirectional policy.

Once within the Mimecast Offshore platform, flexible policy rules enable secure delivery via TLS. Identical policies, available for the receipt of email, may be used to effectively stop sensitive information being sent unencrypted over the internet.

Data that is housed within the Mimecast Message Warehouse is further encrypted with each email uniquely encoded and validated by checksum on entry into the storage grid. The Mimecast Offshore system is therefore able to certify that a client's data has not been modified since it entered the grid. 128 Bit encryption ensures each client's data is effectively unreadable to all but nominated administrators and end users that access the platform through a secure interface. All such access is logged in detail in a forensic event log that is maintained in a highly searchable format.

Mimecast Offshore and Sure International are sometimes required, at the request of the customer or to ensure correct system functioning, to access system data. We are contractually bound to ensure that such access is logged and carefully restricted. However, regardless of this obligation, the system automatically includes all activity in the forensic event log.

The data that we have access to under these controlled conditions is the email metadata (the email header - the To, From, Subject etc), which is essential for the routing of email. At no time whatsoever and under no circumstances do either Sure International or Mimecast Offshore have access to the body content of the email or the attachments. This information is locked down to a "super-user" account that only the client has access to. If a client wanted assistance with a query that involved accessing the body content of an email, the client would be required to provide us with specifically granted rights to do so. We are therefore unable to produce unencrypted data from the system without the client's permission and co-operation.

Summary

The only entity able to disclose any stored information is Sure International's 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 the Channel Islands places an obligation on all Jersey and Guernsey 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 used by Sure International means that the risk of disclosure is virtually nil and that the customer is most likely afforded greater protection in the Channel Islands than in a jurisdiction without such legislation.

eshore

Official Partner of:

sure. International

eShore (Cayman Islands)

Fort Street Building, 2nd Fl.
6 Albert Panton Street
PO Box 2013
George Town
Grand Cayman
KY1-1105
Cayman Islands

+44 1481 757 399
+1 345 946 3673

www.eshoreltd.com