

Data Security

A GENERAL STATEMENT

Although **ByteAccess Limited** is a small company we embrace good business practice wherever possible.

ByteAccess Limited is a small software development company that produces web based business applications for the SME market. All products are based around an ERP system developed by **ByteAccess Limited** and specially designed for SMEs. All products are licensed by **ByteAccess Limited** for use by its clients. Licenses include a support contract that is delivered by telephone, online or onsite visits.

We recognise our responsibilities in respect of data security issues both internally and in respect to the products we license. We have in place a company policy and an action plan regarding Data Security.

ByteAccess Limited is therefore committed to following best data security practice where practical and within the resources available, to mitigate any data security impact that it is responsible for, be it direct or indirect in terms of the company's operation.

ByteAccess Limited wishes to reassure its clients that the security of the data it handles on their behalf is of paramount importance. **ByteAccess Limited** operates a Shared Data Services Centre based in Manchester, which provides the hosting and support of the following services for **ByteAccess Limited**: E-mail (mail boxes, Scanners, Blackberries, Outlook Web Access); Internet hosting of client sites; FTP (File Transfer Protocol) and secure FTP.

The following Data Security statement will give you an overview of the steps we take to safeguard your information. These have been written in addition to our existing policy statements on: Data Protection Act 1998; Information Security; Freedom of Information Act 2000; Business Continuity and Quality Management.

ByteAccess Limited is a registered data user.

SIMON LAMPERT is responsible for all matters relating to Data Security Policy and will, in consultation with all employees, review and revise, where necessary, these statements and the company provisions in place in the light of any issues arising.

STATEMENT OF POLICY

With the help of a Data Security Advisor, the company has assessed what it believes to be the key impacts of the business and has a process of improvements which are outlined as follows:

Operational Impact

ByteAccess Limited will strive to encourage best Data Security practice where possible by:

- ✓ Using strong passwords.
- ✓ Encouraging the changing of passwords at regular intervals.
- ✓ The use of up to date best of breed firewall devices
- ✓ The encryption of all sensitive data stored.

ByteAccess Limited recognises that it is necessary for continued improvement and will constantly look for ways to follow best data security practice as well as encouraging our clients, (through our activities) to focus on data security issues.



Data Security

ByteAccess Limited software and hosted websites

- ✓ Every log-in to [ByteAccess Limited](#) web sites or web applications is registered and the following data are stored and processed temporarily in a 'logbook' file.
 - IP address of the visitor's computer
 - date and time
 - status of login attempt
- ✓ In the case of individual pages being called up, so-called temporary cookies are used to facilitate navigation. Personal data is not registered during this process.
- ✓ Visitors may withdraw their permission for the MFPT to store their personal data at any time.
- ✓ Our website visitors are also entitled to receive information about the storage of their personal data, the origins and receivers of such data, and the purpose of storage. Requests for information may be addressed to the client who owns the web site.
- ✓ All [ByteAccess Limited](#) software components are written to ASP.NET 2.0 standards and every effort is made to minimise the possibility of intrusion by unauthorised users.
- ✓ [ByteAccess Limited](#) strongly recommends the use of security certificates and all clients are offered the opportunity to protect their hosted web sites or web applications using a security certificate (HTTPS). The final decision to use a security certificate rests with the client.

Receiving, transmitting and storing personal data and sensitive personal data

- ✓ [ByteAccess Limited](#) recommends that encryption is the benchmark for transmitting personal data and sensitive personal data. The method of encryption will reflect that required by our clients.
- ✓ [ByteAccess Limited](#) can operate a secure FTP site for the transfer of data between ourselves and our clients.
- ✓ When encryption is not compatible a minimum requirement is to password protect the files to be transferred and to separate the data within a database/ sample file. That means, sending the identifiable data coded in a separate, password protected file that contains a serial number and not name and address details.
- ✓ Where data is transferred by CD/DVD or other mobile storage device, the data should be encrypted. If particularly sensitive we suggest serialising and sending a separate file with the serial number linked to name and address.
- ✓ A secure courier service only must be used and a named receiver given.
- ✓ The sender must check the receipt of the data.
- ✓ We would advise the client to only send information that is relevant to the task in hand. Any additional data should be removed prior to the transfer.

Data Security

Data held within ByteAccess Limited

- ✓ **ByteAccess Limited** operates a highly secure network environment with firewalls, UTM (unified threat management), IDS (intrusion detection system) and Antivirus to ensure no unauthorised access to the network is gained.
- ✓ **ByteAccess Limited** operates tiered storage architecture and data is stored on the appropriate device according to the criticality of the information. A data management policy defines the types of data and where it should be stored and protected depending on the criticality of the data to the business..
- ✓ Access to the data is limited to only those individuals who require it in order to carry out our services for the client.
- ✓ Directories are established to ensure different client data / team directories are logically segregated and all access to files is controlled.
- ✓ Access to information is granted on an as needs basis which has to be authorised by the data owner.
- ✓ All users have a unique User ID and strong password.
- ✓ All data is backed up daily to a secure server in a remote location.
- ✓ No backups are held on mobile storage devices.

Definitions

- ✓ **Personal data:** any information that relates to and identifies a living individual – this can be name, address, post code, job title, email address, recorded image etc.
- ✓ **Sensitive personal data:** race or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, the commission or alleg.
- ✓ **Confidential data:** any other business critical information.

Client Responsibilities under the Data Protection Act

- ✓ Clients must be registered under the Data Protection Act to be able to supply customer data (name/ address/ telephone and other customer details) for “research” purpose.
- ✓ You can check the clients registration at <http://www.esd.informationcommissioner.gov.uk/esd/search.asp>
- ✓ All respondents must have given their permission for their details to be passed on for research purposes – either as an opt-out or opt-in, depending on what method the client has chosen to record this.
- ✓ Clients must record the answers to the above question in such a way that data supplied (whether sample or a data set for data matching purposes) omits the respondents who opt out / have not opted in.
- ✓ Clients need to consider how to respond if any customers query the right to transfer their details to an agency to use for market research purposes.
- ✓ Full details are available from the MRS (www.mrs.org.uk) entitled Market Research Processes (Client) and the Data Protection Act 1998.
<http://www.mrs.org.uk/standards/downloads/revised/legl/mrprocesses.doc>



Company Policy Statement

Data Security

Data Security Assessments

A Data Security Assessment, in consultation with employees, will be undertaken annually by SIMON LAMPERT.

Signed

SIMON LAMPERT

ByteAccess Company Policy