Project	Policies
Document Title	Cloud Solution Provider **–** Customer Data Access Control & Security Policy

Revision History		
Date	**Version**	**Change**
22/09/2017	1.00	New Document
03/10/2017	1.01	Revision to Annex A
10/10/2017	1.02	Clarification on permission terminology
23/10/2017	QMF Issue 1	Assigned QMF number
26/10/2017	QMF Issue 2	Amended Partner Center Users & added signatory section
20/03/2018	QMF Issue 3	Added scope section, Introduction amended to be concise and moved elements to new sections Lines of Responsibility and Data Access and added statement of consequence for non-adherence. Section Related Documents added
25/04/2018	QMF Issue 4	Addition to Partner Centre Users section
28/08/2020	QMF Issue 5	Updated with new Bytes logo

Contents

Introduction

1. The purpose of this document is to detail the extent to which Bytes Software Services can access Customer data as part of their responsibilities as a Cloud Solution Provider, and to document the controls Bytes has put in place to prevent any unauthorised access.

2. This policy is liable to change on a regular basis. Any changes to the list of Bytes employees with access rights will be detailed in Annex A. Any changes to the extent of Bytes access will be listed in the appropriate section and distributed to Customers.

3. Any employee found to have violated these policies may be subject to disciplinary action as set out elsewhere in the Staff Handbook.

4. This policy is in addition to the responsibilities laid out in other Bytes policies, specifically including but not limited to the Information Security and Data Access policies.

Scope

This policy:

- Encompasses all systems that make up the Microsoft Partner Center provided by Microsoft.
- Only applies to aspects of the Microsoft Partner Center that is managed and controlled by Bytes Software Services.

Related Documents

Please also read:

- Information Security Policy
- Data Breach Procedure
- Data Subject Access Request Procedure
- Data Retention Policy

These documents can be found on the Company's Intranet, on the network under the L:\Library\GDPR drive and on the Bytes website: www.bytes.co.uk .

Policy Details

Lines of Responsibility

Signatories of this policy – must ensure that he or she adheres to the content of this policy and enquire from their Manager clarity on any aspect of this policy that is unclear or needs further explanation.

Managers – Managers are responsible for ensuring that signatories of this policy are aware of and comply with this policy.

EXCO – Oversee that this policy is adhered to by Managers and signatories.

Data Access

1. Customer data is private and belongs to the Customer, it does not belong to Bytes Software Services.

2. Accessing Customer data can only be carried out upon receipt of prior written authorisation from the Customer.

3. The signatory of the Customer providing written authorisation must have the responsibility to do so.

4. The written instruction must contain a clear instruction to access the data.

5. Accessing the Customer's data is only carried out to the extent required to complete the specific task.

6. To ensure the security and integrity of the data it should only be accessed from a Bytes provided Laptop, desktop or Citrix environment.

User Subscription Licenses

Definition

1. This section is concerned with Bytes access to Customer data for User Subscription Licenses (USLs).

2. A USL is a license or collection of pre-defined Microsoft services administered through to Office 365 Admin Centre. This includes but is not limited to the Office 365 Enterprise Plans, Power BI, and Project Online.

Native Access Limitations

1. Bytes manage all Microsoft Cloud Agreements through a Microsoft provided online tool called Microsoft Partner Center which grants a limited ability to see Customer data as described in the Microsoft Cloud Agreement.

2. Partner Center Users with any Agent role will have the ability to view a list of Customers' Azure Active Directory Users

3. Partner Center Users with the Admin Agent or Helpdesk Agent will have the ability to conduct "Admin On Behalf Of" actions on customers' Azure Active Directory (AAD) tenant. This is known as Delegated Admin Permissions (DAP).

4. DAP is the same level of AAD tenant access as a Customer User with the Global Admin role and the same restrictions to data access apply, for example:

    a. Bytes will be unable to directly view User, Group, or Shared Mailboxes
    b. Bytes will be unable to directly view SharePoint data
    c. Bytes will be unable to directly view files in OneDrive for Business

5. Office 365 offers a native Audit Logging feature, allowing Customers to interrogate the system for any changes to configuration or permissions. Where this has not already been enabled, Bytes will (at an appropriate time) automatically activate the Audit Logging feature. Bytes would

strongly encourage Customers to configure configuration, access, and permission change Alerts as part of the Audit Logging functionality.

6. Customers may choose to remove Bytes DAP. This will restrict the ability of Bytes Agents' to assist Customers in any support scenario.

Microsoft Azure

Definition

1. This section is concerned with Bytes access to Customer data for Microsoft Azure

2. Azure is Microsoft's public cloud platform.

3. When a customer orders Azure through the Bytes Microsoft Cloud Agreement, Bytes will provision an empty Subscription or Subscriptions, allowing Customers to provision any Azure Consumption Service.

Native Access Limitations

1. Bytes manage all Microsoft Cloud Agreements through a Microsoft provided online tool called Microsoft Partner Center which grants a limited ability to see Customer data as described in the Microsoft Cloud Agreement.

2. Partner Center Users with the Admin Agent or Helpdesk Agent will have the ability to conduct "Admin On Behalf Of" actions in customers' Azure Subscription(s). This is accomplished by Azure recognising all Agents as a single Foreign User Principal with the Azure Role Based Access Control (RBAC) Owner role. This is an inherited role that cannot be removed by the Customer, Bytes, or Microsoft and is the same role granted to the first User that the Customer specifies.

3. The RBAC Owner role allows the download of most stored data types but Customers can enable native AES 256-bit encryption for all stored data and this is a practice that Bytes would strongly encourage.

4. All actions within an Azure Subscription are automatically tracked using the native Audit Logging tool. This can be used to set alerts for all suspicious activity, a practice that Bytes would strongly encourage.

Additional Controls

Administrative Privileges

1. Bytes operates a Policy of Least Privilege for access to any administrative tool or function, including Partner Center. No member of staff will be granted an Agent role in Partner Center unless their tasks cannot be completed using any other functionality.

2. Access to Partner Center is restricted to Users in Bytes Azure Active Directory.

    a. It is Bytes HR Policy that each employee will have only one entry in the Company Active Directory.
    b. Bytes maintains a general IT Policy of a one-to-one relationship between Active Directory and Azure AD through directory synchronisation, utilising Active Directory Federation Services.

c. The addition of Cloud Only Users in Bytes' Azure AD is reviewed and permitted by the Group Head of IT.

d. Any Azure AD administrative privileges are reviewed and permitted by the Group Head of IT.

e. As an extension of Azure AD administrative privileges any Partner Center roles will be permitted by the Group Head of IT after consultation with Bytes Executive Committee and the Bytes Policy of Least Privilege. A list of these Users can be found at Annex A.

f. Changes to any User's administrative permissions in Azure AD, or Partner Center by extension, can only be completed by a Global Admin on Bytes Azure AD that include members of Bytes Systems Support only.

g. All Bytes employees with access to Partner Center will receive training in confidentiality, and this policy specifically, at appointment. Periodic refresher and update training will also be provided where appropriate.

h. All Bytes employees with access to Partner Center will have their privileges reviewed every six months.

Remote Access

1. Due to the nature of Microsoft Partner Center it can be access from any network, however the security of the network it is being accessed from should be considered. Under no circumstances should public wifi's be used.

Arm's Length Systems

1. Most activities that can be completed on Partner Center have a corresponding API, allowing them to be completed using arm's length tools and systems.

2. Bytes have developed a publicly facing portal allowing Customers to create quotes according to pre-defined Vendor pricelists (including Microsoft), request pricing for non-Tier 1 Vendors, and log & track Licensing Service Desk queries (where this feature has been enabled). Bytes employees also use this portal as part of internal process to raise and complete Customer orders.

3. The Partner Center APIs have been integrated in to the Bytes portal to allow employees to raise quotes, and process orders without any direct access to Partner Center. The APIs used for these tasks do not have any effect on Customer environments other than for generating pricing or provisioning services.

4. For any Partner Center tasks that have not yet had an API released by Microsoft, or where the API has not yet been integrated in to the Bytes portal, only the Bytes employees identified in Annex A will complete the work.

Partner Centre Users

The list of Bytes employees with permissible rights to Partner Center, who have read and agreed to these Terms & Conditions, is maintained by the Sales Operations Director.

See "Annex A" for the current list of Bytes employees with permissible rights to Partner Center.

DATA BREACH PROCEDURE

What is Data Breach?

A Personal Data Breach can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

A breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Procedure to Report a Data Breach

As soon as it has become apparent, or suspected, that a personal data breach has occurred, the Company's GDPR Compliance Manager should be notified as soon as possible via gdpr@bytes.co.uk providing as much detail as possible.

On becoming aware of a breach, the Compliance Manager will work with the relevant departmental managers to assess the severity of the data breach and inform the Board. Bytes will try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

Reporting the Data Breach to the ICO

When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms will be established. If it is likely that there will be a risk then the ICO will be notified; if it is unlikely then the ICO need not be informed. Where we decide not to report the breach, it will be documented to justify this decision.

Where Bytes uses a data processor, and the processor suffers a breach, they must inform us without undue delay as soon as they become aware; Bytes will then notify the ICO of the data breach.

ICO: www.ico.org.uk

ICO Reporting Timescales

A notifiable breach will be reported to the ICO without undue delay, but no later than 72 hours after becoming aware of the breach. If it takes longer, then reasons for the delay will be given.

As it is not always possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it, the required information can be provided in phases, as long as it is done without undue further delay.

Information required for the ICO

When reporting a breach to the ICO it will include:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;

- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Notifying the Individual of a Data Breach

The individual will be notified of a breach where it is likely to result in a high risk to the rights and freedoms of the individual.

- When notifying the individual of a data breach, it will be done using clear and plain language and describing the nature of the personal data breach and, at least include:
- the name and contact details of where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Recording of Data Breaches

Regardless of whether or not a data breach was reported to the ICO, all breaches will be recorded. It will record the facts relating to the breach, its effects and the remedial action taken.

Remedial Action of Data Breaches

All breaches will be investigated to establish whether or not it was a result of human error or a systemic issue and see how a recurrence can be prevented; whether that be through better processes, further training or other corrective steps.

Relating Documents

Please also read the Company's Information Security Incident Management Policy.

BYTES

DATA CLASSIFICATION

TYPES OF PERSONAL DATA

- Name
- Surname
- Telephone number
- Mobile number
- Email address
- Physical address
- Work address
- Education (School/College)
- Employee Number
- Gender
- Family details
- Geolocation data
- Vehicle registration number
- Workplace
- Role
- Performance rating
- Employment records
- External Business Interests/Directorships
- Digital Identity
- Travel arrangements
- Postcode
- Grade
- Salary
- Mother's maiden name
- Hotel Booking
- Parent's names
- Loan Information
- Club membership
- Fact of an absence
- Payment information
- Pensions Record
- Drivers License Number
- Passport number & details
- Visa Permit number
- Location at a specific time
- Security questions (user authentication)
- Payroll and Benefits
- IP Address
- Military record
- CRB/DBS record
- Opinions about the individual
- Purchase history
- Gift list
- Delivery details
- Complaints details
- Complaints history
- CCTV images where an individual is recognisable
- Call recording
- Logging details
- Pseudonyms
- Birth Place
- Date of birth
- Cases/Contact History
- Child Data
- Cookies
- Job Role
- National Insurance Number
- Opinions
- Payroll
- Bank details

TYPES OF SPECIAL CATEGORY DATA

- Genetic Information
- Membership of trade union
- Private healthcare
- Additional Private healthcare
- Measurements (feet, body)
- Reasons for absences
- Biometric
- Sex life
- Dietary requirements
- Ethnicity
- Health Records
- Insurance Data
- Religion
- Disability Information
- Sexual Orientation
- Philosophical beliefs
- Political opinions
- Health adjustments

DATA RETENTION POLICY

The purpose of this Policy is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed, or are of no value, are discarded at the proper time. This Policy applies to all members of staff and third parties that perform development of systems owned by Bytes Software Services (“Bytes”).

Records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organisation operates with in statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status or an organisation to shareholders, external parties and auditors. National law or regulation may set the time period and data content for information retention.

We have assessed our records to:

- Determine their value as a source of information about Bytes, its operations, relationships and environment
- Assess their importance as evidence of business activities and decisions
- Establish whether there are any legal or regulatory retention requirements

In some instances, this Data Retention Policy may be temporarily suspended, specifically if an investigation, court case, or audit is anticipated. In some instances, this policy’s Data Retention schedule may conflict with the need to produce documents relevant to the aforementioned legal or regulatory procedures. If this is the case, then the need to comply fully with the law and/or regulation will override this policy, causing this policy to be temporarily suspended until the matter in question is satisfactorily resolved. Suspension of this policy will take the form of no business documents being disposed of whatsoever for a period of time.

The Company’s Data & Records Retention Schedule is maintained by the GDPR Compliance Manager.

GENERAL IT POLICY

Introduction
The Policy document serves as confirmation that Bytes Software Services (“Bytes”) has an IT User Policy* which is a condition of employment and rolled-out to all new starters at Induction, and to all employees on an annual basis to ensure the effective protection and proper usage of the computer systems within Bytes. Any employee found to have violated the IT User Policy may be subject to disciplinary action. The IT investment of the organisation is considerable and the dependency on computer technology in the delivery of Bytes’ services is high.

Policy Details
The IT User Policy covers the following topics:

- Lines of Responsibility
- Review of Policy
- Service Desk
- Computer Systems including Network, Hardware (PCs, Laptops, Notebooks, etc.), and Personal Devices
- Software & Software Applications
- Data / Electronic Information
- Back-up
- Anti-Virus Protection
- Encryption
- Software Auditing
- Computer Users including Health & Safety, Training, User Accounts, Passwords, System Usage, and Saving Documents
- E-mail, Internet, and Instant Messaging
- Mobile Phones
- Telephones
- Service Levels
- Copyright Infringement / Piracy Policy
- Contravention of the Policy

Related Documents
Please also read:

- Backup Policy
- Data Breach Procedure
- Data Subject Access Request Procedure
- Data Retention Policy
- Information Security Policy

* Internal document only

Document ID	POL002
Document Title	Information Security Incident Management Policy
Author	Kevin Beadon
Version	1.10

Revision History		
Date	Version	Change
28/09/2017	1.00	New Document
08/06/2020	1.10	Annual review

Distribution		
Date	Version	Distribution
28/09/2017	1.00	Sara Mitchell (DPC)
28/09/2017	1.00	All staff via Intranet and Library
08/06/2020	1.10	All staff via Intranet and Library

Signed			
Date	Version	Name	Role
28/09/2017	1.00	N/A	N/A
08/06/2020	1.10	Keith Richardson	CFO

Next Review: 08/06/2021

Contents

Introduction

The specific purpose of this policy is to ensure consistent management of information security incidents to minimise any harm to individuals or organisations. This policy is not intended to consider the impact and protection of the company's assets from accidents, such as fire, flood, failed hardware or software.

This policy provides the necessary information for the management and reporting of:

- Security incidents affecting Bytes Software Services and IT systems
- Loss of information
- Near misses and information security concerns

Intended Audience

This policy applies to all:

- Employees of Bytes Software Services, including senior and executive management
- Contractors that make use of Bytes Software Services IT facilities
- IS Manager, IT Manager or Manager responsible for any element of Bytes' IT Systems

Policy Details

Overview

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of Bytes information in any format.

Examples of information security incidents can include, but are not limited to, the following:

- Disclosure of confidential information to unauthorised individuals
- Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- Inappropriate access controls allowing unauthorised use of information
- Suspected breach of Bytes' IT policy
- Attempts to gain unauthorised access to computer systems, e.g. hacking
- Records altered or deleted without authorisation by the data "owner"
- Virus or other security attack on IT equipment, systems or networks
- Breaches of physical security e.g. forcing of doors or windows into secure room, or opening filing cabinets containing confidential information left unlocked in accessible area
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information
- Covert or unauthorised recording of meetings and presentations

Lines of Responsibility

All users who are given access to Bytes information, IT and communications facilities are responsible for reporting any actual or potential breach of information security promptly in line with Reporting an Incident.

All users are responsible for identifying risk to information security and ensuring that it is reported accordingly. The user reporting the incident or appropriate person may then be asked to assist with investigating and mitigating the risk. Any breach should be reported to the Group Head of IT (or equivalent) immediately

Group Head of IT (or equivalent) is responsible for leading the activity required to respond to an incident. Activities include reporting to the Financial and Operations Director and the Data Protection Co-ordinator, investigating and taking appropriate action to address breaches of IT systems and network security, and for escalating incidents to the Financial and Operations Director (or equivalent) and the Data Protection Co-ordinator

Financial and Operations Director (or equivalent) has Board level responsibility for reporting any serious information security breach to EXCO and ensuring that appropriate actions are taken to address the breach.

Data Protection Co-ordinator is responsible for ensuring that new systems meet the requirements of GDPR and therefore have had information security considered during deployment and on-going management. Has responsibility for ensuring that reporting to relevant people in the business, and appropriate actions are taken to address breaches. May be required to report breaches to third parties.

Account Managers are responsible for reporting any breaches to affected customers or third parties

Review of Policy

Group Head of IT (or equivalent), Financial and Operations Director (or equivalent) and Data Protection Co-ordinator are responsible for reviewing the Information Security Incident Management Policy annually or after a serious and significant breach.

Reporting an Incident

An incident should be reported using any of the following methods:

- E-mail helpme@bytes.co.uk
- Call 01372 418504
- Web https://helpme.bytes.co.uk
- Visit the Systems Support team in Leatherhead

When an incident is reported it will be entered into the Company's call logging system, and the Group Head of IT will be informed. The breach will be categorised as follows:

Serious breach includes, but not limited to, loss or potential loss of personal data about a Bytes employee, customer or supplier and/or the transfer of personal data to unauthorised third parties

Significant breach includes, but not limited to, loss or potential loss of non-personal customer data that Bytes host

Other breach includes, but not limited to, loss or potential loss of non-personal data

If the breach is categorised as 'serious' or 'significant' the Finance & Operations Director will be informed. All information security breaches are reported to the Data Protection Co-ordinator. If necessary, the Data Protection Co-ordinator will report the breach to the relevant Bytes Account Manager who will then inform their affected customer

Representatives of the Group Head of IT looking into security breaches will be responsible for updating, amending and modifying the status of incidents in the Company's Service Desk system.

Acting on an Incident

All parties dealing with security incidents shall undertake to:

- Analyse and establish the cause of the incident and take any necessary steps to prevent recurrence;
- Report to all affected parties and maintain communication and confidentiality throughout investigation of the incident;
- Identify problems caused as a result of the incident and to prevent or reduce further impact;
- Contact 3rd parties to resolve errors/faults in software and to liaise with the relevant departmental personnel to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Bytes systems and services;
- Ensure all system logs and records are securely maintained and available to authorised personnel when required;
- Ensure only authorised personnel have access to systems and data;
- Ensure all documentation and notes are accurately maintained and recorded in the Company's Service Desk system and are made available to relevant authorised personnel;
- Ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness;
- The Data Protection Co-ordinator will maintain a log of all security breaches;

- Serious incidents will be presented to EXCO;
- Serious breaches will need to be reported to the Information Commissioner by the Data Protection Co-ordinator;
- All incidents logged within the Company's Service Desk system shall have all details of the incident recorded including any action/resolution, links or connections to other known incidents. Incidents which were initially resolved but have recurred will be reopened or a new call referencing the previous one will be created;
- Monthly reports on incidents generated by the Service Desk system are automatically sent to the Group Head of IT to facilitate the monitoring of the types, numbers, frequency and severity of incidents which will help to correct and prevent incidents recurring;
- During the incident investigations, hardware, logs and records may be analysed by Bytes' internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential that confidentiality is maintained at all times during these investigations.

BYTES

Document ID	POL009
Document Title	Backup Policy
Author	Kevin Beadon
Version	1.50

Revision History		
Date	Version	Change
25/01/2018	1.00	New Document
26/01/2018	1.10	Minor updates after Paul Wheaton review
26/01/2018	1.20	Minor updates after Keith Richardson review
31/01/2018	1.30	Minor updates after Sara Mitchell review
02/09/2019	1.40	Minor update to include copy of data to a non-Microsoft filesystem and statement of encryption.
08/06/2020	1.50	Annual review

Distribution		
Date	Version	Distribution
25/01/2018	1.00	Paul Wheaton
26/01/2018	1.10	Keith Richardson, Sara Mitchell
26/01/2018	1.20	Keith Richardson, Sara Mitchell
31/01/2018	1.30	All staff via Intranet & Library drive
02/09/2019	1.40	Keith Richardson, Sara Mitchel
19/09/2019	1.40	All staff via Intranet and Library
08/06/2020	1.50	All staff via Intranet and Library

Signed			
Date	Version	Name	Role
25/08/2018	1.00	N/A	N/A
08/06/2020	1.50	Keith Richardson	CFO

Next Review: 08/06/2021

Contents

Introduction

The purpose of this Policy is to:

- To safeguard the information assets of Bytes Software Services (Bytes/Company).
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time defined by system backup policies.

Backup retention periods are in contrast to data retention periods defined in the GDPR Data Register

System backups are not meant for the following purposes:

- Archiving data for future reference.
- Maintaining a versioned history of data.

Scope

This Policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by Bytes and applies to all servers and data (on-premise or cloud) that is managed by Bytes.

Policy Details

Overview

This Policy is set out to identify how Bytes Software Services safeguards important information in case of data loss, etc and to outline frequency and how long backups are retained.

Lines of Responsibility

All users – Ensuring that data stored on Bytes-provided devices such as laptops is copied to the File Servers ready for backup. Data on user devices are not backed-up unless copied to Bytes File servers.

Systems Support Team is responsible to the Group Head of IT and they:

- Ensure facilities are available.
- Ensure sufficient backup space is available.
- Take overall responsibility for trust adherence to this Policy.
- Check the backup log for completion, be responsible for the safekeeping and availability of all back-up media and logs.
- Perform test/live restores.
- Report any backup failures to the Group Head of IT and log accordingly and investigate any reported exceptions.

Group Head of IT (or equivalent) is responsible for ensuring that the backup Policy is adhered to and any new systems follow this Policy. Escalation is to the Financial and Operations Director (or equivalent).

Finance and Operations Director (or equivalent) has Board level responsibility for ensuring that Bytes Software Services data is backed-up according to the business need.

Review of Policy

Group Head of IT (or equivalent) and the Financial and Operations Director (or equivalent) are responsible for reviewing the backup Policy annually or after a serious issue.

Systems Backup

Bytes has the following types of backup data:

- File Server – Unstructured data located on Bytes fileservers
- E-Mail – E-mail data stored on-premise on Exchange 2016
- Database – All structured data contained on database
- SharePoint – Unstructured data stored on Azure Cloud service
- Virtual Machine – All data stored on a virtual server including the Operating System and data

Backup details of the various backup data types:

- File Server
    - Frequency: Daily
    - What is backed up: Changed data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - After 60 days backup is rolled-up to one full 30-day backup
        - Each 30-day full backup is retained for 12 months (12 x Monthly backups)
- E-mail
    - Frequency: Daily
    - What is backed up: Changed data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - After 60 days backup is rolled up to one full 30-day backup
- Database
    - Frequency: Daily
    - What is backed up: Full data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - After 60 days backup is rolled-up to one full 30-day backup
        - Each 30-day full backup is retained for 12 months (12 x Monthly backups)
- SharePoint
    - Frequency: Daily
    - What is backed up: Changed data
    - Retention:
        - Minimum of 30 days and Maximum of 60 days
        - Each 30-day full backup is retained for 12 months
- Virtual Machines
    - Frequency: Snapshot every 4 hours
    - What is backed up: Changed data
    - Retention:
        - 2 days

Exceptions are as follows:

- Door Entry System (SQL)
    - Frequency: Monthly
    - What is backed up: All data in the SQL database
    - Retention:
        - 2 Months

Transportation and Storage of Backup

- All production backup data is stored at Bytes Leatherhead office and off site at the DR datacentre, Croydon.
    - Exceptions are the 12 monthly backups which are stored at the DR datacentre only
- All backup data is written to disk
- A copy of the backup data is made on a non-Microsoft file system
- File, E-mail, SQL backup data is maintained by Attix Backup system
- Attix backup is encrypted in transport and at rest using AES256
- SharePoint is backed-up using Metalogix from Azure to File server and then treated as a file backup.
- Virtual Machine backups are maintained using NetApp SnapMirror.
- All data is transported to the DR datacentre across encrypted VPN.
- File, E-mail, SQL and SharePoint data is stored on the production datacentre for a minimum. of 30 days and a maximum of 60 days. All other backup data is located off site at the DR datacentre only.
- All Virtual Machine backup data is located at the production and DR datacentre.
- Expired backup data is deleted automatically.

Disposal of Media

Bytes Software Services only store data on disk and therefore the backup media is regarded as the disks storing the backup data.

- Prior to retirement and disposal, Systems Support will ensure that:
    - The media no longer contains active backup images.
    - The media's current or former contents cannot be read or recovered by an unauthorised party.
- Backup media (the disk storage holding the backup data) is destroyed and recycled in accordance with the Waste, Electrical and Electronic Equipment Directive 2012/19/EU and records maintained.

Validation

- Daily, logged information generated from each backup job will be reviewed for the following purposes:
  - To check for, and correct, any errors.
  - To monitor the duration of the backup job.
  - To optimise backup performance where possible.
- Systems Support will identify problems and take corrective action to reduce any risks associated with failed backups.
- Random test restores from the production datacentre will be carried out once a month to verify that backups have been successful
- Random test restores from the DR datacentre will be carried out once every three months to verify that offsite backups are valid
- IT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this Policy for auditing purposes.

Data Recovery

- Requests for data recovery is made using any of the following methods:
  - E-mail helpme@bytes.co.uk
  - Call 01372 418504
  - Web https://helpme.bytes.co.uk
  - Visit the Systems Support team in Leatherhead
- Systems Support aim to perform data restore requests within 1 working day.

Document ID	POL010
Document Title	Information Security Policy
Author	Kevin Beadon
Version	1.50

Revision History		
Date	Version	Change
05/02/2018	1.00	New Document
05/02/2018	1.10	Update after Paul Wheaton Feedback
07/02/2018	1.20	Update after Sara Mitchell Feedback
04/09/2019	1.30	Update to reflect ISO270001 requirements
04/12/2019	1.40	Updated to reflect POL019 – Network Systems Monitoring Policy
08/06/2020	1.50	Annual review

Distribution		
Date	Version	Distribution
05/02/2018	1.00	Paul Wheaton, Sara Mitchell
05/02/2018	1.10	Paul Wheaton, Sara Mitchell
07/02/2018	1.20	Paul Wheaton, Sara Mitchell, Keith Richardson
12/02/2018	1.20	All Staff via Intranet and Library Drive
04/09/2019	1.30	Keith Richardson, Sara Mitchell
18/09/2019	1.30	All Staff via Intranet and Library Drive
04/12/2019	1.40	Keith Richardson, Sara Mitchell
19/12/2019	1.40	All Staff via Intranet and Library Drive
08/06/2020	1.50	All Staff via Intranet and Library Drive

Signed			
Date	Version	Name	Role
05/02/2018	1.00	N/A	N/A
08/06/2020	1.50	Keith Richardson	CFO

Next Review: 08/06/2021

Contents

Introduction

The purpose of this policy is to:

- Define the information security standards of Bytes Software Services (Bytes/Company).
- Establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Bytes Software Services.
- Protect from all threats, whether internal or external, deliberate or accidental the information assets of:
    - Bytes
    - Customers
    - Suppliers

Objectives and Goals

The implementation of this policy is important to maintain and demonstrate our integrity in our dealing with customers and suppliers.

It is the policy of Bytes to ensure:

- Information is protected against unauthorised access
- Confidentiality of information is maintained
- Information is not disclosed to unauthorised persons through deliberate or careless action
- Integrity of information through protection from unauthorised modification
- Availability of information to authorised users when needed
- Regulatory and legislative requirements will be met
- Business continuity plans are produced, maintained and tested as far as practicable
- Information security training is given to all employees
- All breaches of information security and suspected weaknesses are reported and investigated

It is the objectives of Bytes to:

- To continually strengthen and improve the overall capabilities of the information security management system.
- To increase professional skills in terms of information security management and technology.
- To make Bytes' management system for information security so complete and reliable that the ISO/IEC 27001 certification standard will continue to be effective.
- To ensure that information-related business operations continue to be carried out in line with the ISO/IEC 27001 standard and to establish a sustainable operation plan for the business that is cost-effective.
- To establish quantified information security goals annually through management and review meetings.

Supporting Policies

The following documents support this policy:

- POL001 - Firewall Policy
- POL002 – Information Security Incident Management Policy
- POL003 – Incident and Problem Management Policy
- POL005 – Software Patching – Internal Systems Policy
- POL006 – Software Patching – Snow Systems Policy
- POL008 – Malware Incident Management Policy
- POL009 – Backup Policy
- POL011 – IT User Policy
- POL012 – Remote Access Policy
- POL013 – Change Management Policy
- POL014 – User Management Policy
- POL015 – Servers Access Policy
- POL016 – Cryptographic Controls Policy
- QMF 41 – Business and Continuity Management Strategy and Policy
- POL017 – Remote Access and Teleworking Policy
- POL018 – Access Policy
- POL019 – Network Systems Monitoring Policy

Scope

This policy, and supporting procedures, encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by Bytes. It covers the following areas:

- Users access and controls.
- Resource access logs and violation reporting.
- General classification of data.
- Basic data protection requirements.
- Storage media.
- Data transfer.
- Information awareness training.
- Responsibilities for information Security.
- Physical security of IT equipment.
- Terminated employees.
- Accessing customer data

Policy Details

Overview

This policy sets out the policies for information security and how it is applied to Bytes.

Lines of Responsibility

All users – Are responsible for:

- Complying with information security policy and procedure.
- The operation security of the information systems they use.
- Complying with the security requirements that are currently in force.
- Ensuring the confidentiality, integrity and availability of the information they use and that it is maintained to the highest standard.

Information owners (Managers) are responsible for:

- Helping with the security requirements for their specific area.
- Determining the privileges and access rights to the resources within their areas.

Systems Support Team is responsible to the Group Head of IT and they:

- Ensure the implementation and operation of IT security.
- Ensure the implementation of the privileges and access rights to the resources.
- Support information security policies.

Group Head of IT (or equivalent) is responsible for:

- The security of IT infrastructure.
- Planning against security threats, vulnerabilities and risks.
- Implementing and maintaining the information security policy document(s).
- Ensuring IT infrastructure supports the information security policy.
- Responding to information security incidents.
- Systems Disaster Recovery plans.
- Validating security training plans.

Finance and Operations Director (or equivalent) has Board level responsibility for Information Security within Bytes Software Services.

Review of Policy

Group Head of IT (or equivalent) and Financial and Operations Director (or equivalent) are responsible for reviewing the Information Security Policy annually or after a serious issue.

User Access and Controls

- Any system that handles valuable information must be protected with a password-based access control system.
- Every user must have a separate, private identity for accessing IT network services.

- Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
- Discretionary access control list must be in place to control the access to resources for different groups of users.
- Cloud services must support SAML2 and authenticate to the Bytes Office 365 tenant
  - When access outside of the Bytes internal network MFA must be used
- Mandatory access controls should be in place to regulate access by processes operating on behalf of users.
- Access to resources should be granted on a per-group basis rather than on a per-user basis.
- Access shall be granted under the principle of "least privilege", i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform their business functions.
- Whenever possible, access should be granted to centrally defined and centrally managed identities.
- Users should refrain from trying to tamper or evade the access control to gain greater access than they are assigned.
- Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls.
- Using administrative credentials for non-administrative work is not allowed.
- IT administrators must have two set of credentials: one for administrative work and the other for everyday work.
- Test accounts are allowed but cannot be used for Administrative or everyday work and should be deleted as soon as they are no longer required.

Password

Passwords must meet the following complexity requirements:

- Each identity must have a strong, private, alphanumeric password to be able to access any service. They should be as least 8 characters long.
- Administrative passwords must be at least 10 characters long.
- Each regular user may use the same password for no more than 40 days and no less than 3 days.
- A password history of at least 10 passwords must be kept
- Password for some special identities will not expire. In those cases, password must be at least 12 characters long.
- Whenever a password is deemed compromised, it must be changed immediately.
- Sharing of passwords is forbidden. They should not be revealed or exposed to public sight.
- Identities must be locked if password guessing is suspected on the account.

Resource access logs and violation reporting

- Systems should report successful and unsuccessful log on attempts.
- Systems Support will maintain a process for searching audit logs.

General Classification of Data

All data within Bytes Software Services is regarded as business confidential unless otherwise stated.

Business confidential data:

- Should not be shared with people outside of the organisation without prior approval by EXCO.
- Should only be shared within the business on a least privilege model.
- Should only be stored on Bytes controlled systems.
- Should be secured by an individual user ID and Password.

Special category data:

- Is only stored by HR and located within the HR System or on the HR area of the file server.
- Access is given on a least privilege model and authorised by HR or EXCO only.

See Data Classification document L:\GDPR\Data Classification.pdf for details

Basic Data Protection Requirements

All Bytes Software Services controlled systems containing personal information as defined in the Data Classification document must be protected in alignment with corporate standards and best practice.

Specifically, where a system is in the:

- Production and DR datacentre.
- Bytes Software Services office corporate network.

A system must operate:

- Up to date anti-malware.
- Be appropriately patched.

Where a system (including laptops and mobile phones) is operated outside of these environments the device must also operate:

- Encryption.

Storage media

Backups must be encrypted in line with industry best practice and hosted in a physical secure environment to protect against loss. Backup media must be stored in one of the following locations:

- Leatherhead datacentre.
- DR datacentre.
- Inside a locked fire safe located within a Bytes Software Service office.

Only Systems Support approved USB memory drives/stick or similar type devices are to be used on Bytes servers.

Media that is used to store Bytes data must be returned to the Systems Support for destruction, this includes but limited to servers' hard disks, USB drives, laptops and desktops.

Any media that will be reused outside of Bytes must have their media wiped to UK Government standards.

Data transfer

Data transfer containing personal, business confidential or special category data must follow either of the following rules:

- When transferred outside of the organisation on a network it must be via secure mechanisms such as TLS or the data must be encrypted.
- When transferred on a portable device such as a flash drive or laptop outside of the organisation it must be encrypted.

Information awareness training

- Information security training must be given to all staff during their induction.
- Ongoing training must be given at regular intervals to ensure that all staff are aware of current policies.

Physical Security of IT Systems

IT Systems that store data or provide access to data must be in a server room:

- That is locked and controlled separately by key card.
- That has environmental monitoring and alerting.
- Where access to the server room is logged and a reason recorded.
- Where access is by authorised personnel only.
- That is in an area not open to the general public.
- Within a building that has CCTV.
- That has UPS.
- That has a generator.
- That has air conditioning.

IT Systems that are in remote offices can only be used for authentication, routing of network or storing non-personal data other than personal data that is required for authentications purposes. These IT Systems must be in a server room:

- That is locked.
- That has environmental monitoring and alerting.
- Where access is by authorised personnel only.
- That is in an area not open to the general public.

Terminated Users

A terminated user includes all users that are no longer employed or contracted by Bytes Software Services. On a user's last day, the following must be executed or configured:

- The terminated users account(s) must have the password changed.
- All access to IT Systems will be revoked.
- All Bytes Software Services IT supplied equipment must be returned.
- If for any reason the user is keeping Bytes supplied IT equipment it must be reset to factory settings, all data securely erased and logged as now owned by the terminated user.
- Further access to Bytes Software Services buildings will be as a visitor and they must be escorted.

PRIVACY POLICY AND COOKIE NOTICE

Bytes Technology Group was formed in 1982 and is one of the largest software services and solutions businesses in the UK. Registered in England and Wales under company number 03643194, the company is the holding company for Bytes Software Services Limited and Phoenix Software Limited (collectively known as "Bytes"). This Privacy Policy and Cookie Notice incorporates all three subsidiary companies.

Bytes provide security, cloud management, software licensing, software asset management, data storage, training, consultancy services and information security professional services & assurance testing. Bytes has its registered office address at Bytes House, Randalls Way, Leatherhead, Surrey, KT22 7TW and is a subsidiary of Allied Electronics t/a Altron based in South Africa.

Bytes operate the following websites: www.bytes.co.uk; www.phoenixs.co.uk and www.licensedashboard.com.

GDPR Principles

The following principles are complied with when processing personal data:

- Data is processed fairly and lawfully
- Data is processed only for specified and lawful purposes
- Processed data is adequate, relevant and not excessive
- Processed data is accurate and, where necessary, kept up to date
- Data is not kept longer than necessary
- Data is processed in accordance with an individual's consent and rights
- Data is kept secure
- Data is not transferred to countries outside of the European Economic Area ('EEA') without adequate protection

Lawful Basis of Processing Data

The lawful basis of processing of data will always be determined prior to any data being processed. Bytes processes personal data under one, or more, of the following Lawful Bases in accordance with GDPR:

- **Consent** – the individual has given their Consent to the processing of their personal data
- **Contractual** – processing of personal data is necessary for the performance of a contract to which the individual is a party, or for Bytes to take pre-contractual steps at the request of the individual
- **Legal Obligation** – processing of personal data is necessary for compliance with a legal obligation to which Bytes is subject
- **Legitimate Interests** – processing of personal data is necessary under the Legitimate Interests of Bytes or a Third Party, unless these interests are overridden by the individual's interest or fundamental rights

Type of Personal Data collected

The type of personal data collected may include:

Name
Address
Email address
Job Title
Telephone number
Business name
IP address
Demographic information such as postcode

How Personal Data is collected

Personal data is obtained from one or more of the following:

Visits and use of the above Bytes websites, and Company Portals
Use of Bytes' social media
Use of Google Analytics
Attendees of corporate seminars and webinars hosted by Bytes
Subscribers to Bytes Company updates
Parties entering into agreements with Bytes
Requests for information about products and services offered by Bytes, and/or quotes
Employment enquiries

Why Personal Data is collected

Personal data is collected to provide legitimate business services which include:

For Marketing purposes
For us to review and reply to your enquiry
To provide an opinion for a service you have requested
To meet our statutory monitoring and reporting responsibilities
To handle and communicate orders, billings and payment, delivery of products and services
To improve Bytes' services and product offering

However, where indicated, some of the information is optional and you can choose not to complete.

How Personal Data is used

Personal data may be used to:

- process orders, process a request for further information, to maintain records and to provide pre and after-sales service.
- pass to another organisation to supply/deliver products or services you have purchased and/or to provide pre or after-sales service;
- pass onto our partners in order to follow-up on any webinars & events that you have registered for;
- carry out our obligations arising from any contracts entered into by you and us;
- carry out security checks (this may involve passing your details to our Identity Verification partners, who will check details we give them against public and private databases - this helps to protect us from credit risk and both you and us from fraudulent transactions);
- comply with legal requirements;
- assist third parties to carry out certain activities, such as processing and sorting data, monitoring how customers use our site and issuing our emails for us;
- seek your views or comments on the services we provide;
- notify you of changes to our services;
- send you communications which you have requested and that may be of interest to you. These may include information about product updates, newsletters, events, webinars;
- inform you of various promotions, goods and services that may be of interest to you. You may be contacted by post, email, telephone, SMS or such other means with carefully selected marketing communications we deem relevant to send to you in the legitimate interests of Bytes as an IT service provider. Each marketing communication sent to you by Bytes will provide you with the option to unsubscribe and manage your data profile and communication preferences from Bytes at any time;
- process a job application;
- create a profile of your interests and preferences so that we can contact you with information relevant to you. We may make use of additional information about you when it is available from external sources to help us do this effectively.

Where Personal Data is Stored

Information collected is stored on the Company's CRM system.

As part of any services offered by Bytes, information provided may be transferred to countries outside the European Economic Area ('EEA') i.e. our servers, or third party servers that are used to provide Bytes services located in a country outside the EEA. By submitting your data, you consent to the transfer, storage and/or processing of your data wherever it be stored. However, if your data is transferred outside the EEA, steps will be taken to ensure appropriate security measures are in place to ensure your privacy rights continue to be protected as outlined in this Policy.

Bytes websites - Previous browsing history is available to Bytes employees only, to determine your interests in order that we can engage with you more effectively and improve our site. If Cookies are switched off then your previous browsing history is no longer be available to Bytes (See "Cookies" below). If you do not wish for us to have your personal information, please do not fill out any of the web forms on these sites.

Livechat (https://www.livechatinc.com/) provides our webchat functionality. Data provided via this system may be stored on servers based in the United States under a "Privacy Shield". This means that the data will be managed to similar standards to those required under GDPR.

How long Personal Data is stored

We review our retention periods for personal data on a regular basis. We are legally required to hold some types of information to fulfil our statutory obligations. We will hold personal data on our systems for as long as is necessary for the relevant activity, or as long as is set out in any relevant contract you hold with us.

Who has access to Personal Data

Only Bytes employees are granted access to customer data. This is ensured by the use of strict operational processes and procedures.

Staff are trained on security systems and relevant processes and procedures which are reviewed regularly for ongoing effectiveness and suitability for purpose. All employees are kept up-to-date on the Bytes security and privacy practices. Employees are notified and/or reminded about the importance we place on privacy, and what they can do to ensure that customer information is protected.

Personal data provided via the Company's portals is secured using Secure Socket Layer (SSL) server and is encrypted before being transmitted. Secure pages have a lock icon or key on the bottom of web browsers such as Microsoft Internet Explorer, information supplied by you on these webpages is securely stored and can only be accessed for the purposes for which it was provided.

All IT systems are kept in a secure environment with appropriate access control. We are audited on a regular basis by various independent security companies, plus internal audits by the Company's Parent company.

Non-sensitive details (your email address and other requested information) are transmitted normally over the Internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

We will not sell or rent your information to third parties.

Third Party Service Providers working on our behalf:

> We may pass your information to our third party service providers, agents, subcontractors and other associated organisations for the purposes of completing tasks and providing services to you on our behalf. However, when we use third party service providers, we disclose only the personal information that is necessary to deliver the service and we have a contract in place that requires them to keep your information secure.

Third Party Product Providers we work in association with:

> We work closely with various third party product providers to bring you a range of quality and reliable products and services designed to meet your needs. When you enquire about or purchase one or more of these products, the relevant third party product provider will use your details to provide you with information and carry out their obligations arising from any contracts you have entered into with them. In some cases, they will be acting as a data controller of your information and therefore we advise you to read their Privacy Policy. These third party product providers will share your information with us which we will use in accordance with this Privacy Policy.

We may transfer your personal information to a third party as part of a sale of some or all of our business and assets to any third party including for a merger, acquisition, divestiture, or similar transaction or as part of any business restructuring or reorganisation.

We may also further transfer data if we are under a duty to disclose or share your personal data in order to comply with any legal obligation or to law enforcement. However, we will take steps with the aim of ensuring that your privacy rights continue to be protected.

Individuals' Rights

Different rules apply depending on the type of Lawful Processing being undertaken, however many of the following individuals' rights apply whatever the basis of processing:

- The right to be informed how personal data is processed
- The right of access to their personal data
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

The accuracy of personal data is imperative. We aim to keep it updated at all times. The personal data we hold on you is available upon request by contacting GDPR@bytes.co.uk. You can request that your data is updated and/or deleted at any time, unless Bytes can justify that it is retained for legitimate business or legal purpose. When updating your personal data, you may be asked to verify your identity before your request can be actioned.

You can change your marketing preferences at any time by calling our switchboard on 01372 418500, or by emailing tellmemore@bytes.co.uk, or by clicking on the "Unsubscribe" link at the bottom of any of Bytes e-shots.

Links to other websites / from other websites

Bytes websites may contain links to other websites run by other organisations. Bytes Privacy Policy only applies to Bytes' websites and you are encouraged to read the Privacy Statements on the third party websites that you visit such as *Google*. Bytes is not responsible for the Privacy Policies and practices of other websites even if they were accessed via a Bytes website. Equally, if you link to a Bytes website from a third party site, Bytes is not responsible for the Privacy Policies and practices of that third party site.

16 or Under

We are concerned to protect the privacy of children aged 16 or under. If you are aged 16 or under, please get your parent/guardian's permission beforehand whenever you provide us with personal information.

COOKIES

What are cookies?

A cookie is a text file containing small amounts of information which a server downloads to your personal computer (PC) or mobile device when you visit a website. The server then sends a cookie back to the originating website each time you subsequently visit it, or if you visit another website which recognises that cookie.

Why do websites use cookies?

Web pages have no memory. If you are surfing from page to page within a website, you will not be recognised as the same user across pages. Cookies enable your browser to be recognised by the website. So cookies are mainly used to remember the choices you have made – choices such as the language you prefer and the currency you use. They will also make sure you are recognised when you return to a website.

Do all cookies do the same thing?

No, there are different types of cookies and different ways of using them. Cookies can be categorised according to their function, their lifespan and according to who places them on a website.

How does Bytes use cookies?

Our website uses the following types of cookie:

Technical cookies: We try to give our visitors an advanced and user-friendly website that adapts automatically to their needs and wishes. To achieve this, we use technical cookies to show you our website, to make it function correctly. These technical cookies are absolutely necessary for our website to function properly.

Functional cookies: We also use functional cookies to remember your preferences and to help you to use our website efficiently and effectively, for example by remembering your preferred currency and language that you viewed earlier. These functional cookies are not strictly necessary for the functioning of our website, but they add functionality for you and enhance your experience.

Analytics cookies: We use these cookies to gain insight into how our visitors use the website, to find out what works and what doesn't, to optimise and improve our website and to ensure we continue to be interesting and relevant. The data we gather includes which web pages you have viewed, which referring/exit pages you have entered and left from, which platform type you have used, date and time stamp information and details such as the number of clicks you make on a given page, your mouse movements and scrolling activity, the search words you use and the text you type while using our website. We also make use of analytics cookies as part of our online advertising campaigns to learn how users interact with our website after they have been shown an online advertisement, which may include advertisements on third-party websites. We will not know who you are, and only obtain anonymous data.

Commercial cookies: We use these to show you Bytes advertisements on other websites. This is called "retargeting" and it aims to be based on your browsing activities on our website, such as the destinations you have been searching for, the products you have viewed and the prices you have been shown.

How long do Bytes cookies stay active?

The cookies we use have varying lifespans. The maximum lifespan we set on some of them is five years from your last visit to our website. You can erase all cookies from your browser any time you want to.

How can you recognise Bytes cookies?

You can find our cookies in your browser settings.

Does Bytes use third-party cookies?

Yes, Bytes uses the services of trusted and recognised online advertising and marketing companies. Bytes may also use third-party providers for analytical purposes. To enable their services, these companies need to place cookies.

The providers we use are committed to building consumer awareness and establishing responsible business and data management practices and standards.

When it comes to online advertising and marketing companies, we strive to only work with companies that are members of the Network Advertising Initiative (NAI) and/or the Interactive Advertising Bureau (IAB). Members of NAI and IAB adhere to industry standards and codes of conduct. NAI and IAB members allow you to opt out of the behavioural advertising.

Visit www.networkadvertising.org and www.youronlinechoices.com to identify the NAI members that may have placed an advertising cookie file on your computer. To opt out of an NAI or IAB member's behavioural advertising programme, simply check the box that corresponds to the company from which you wish to opt out.

In order to control the collection of data for analytical purposes by Google Analytics, you may want to visit the following link: https://tools.google.com/dlpage/gaoptout

Use of re-targeting functions on the website

Activation of interest-related advertising using "re-targeting". All Bytes websites use "re-targeting Tags" which is a JavaScript element positioned in the website source code. When a user visits a page that contains a re-targeting tag, the provider of the online advertising (e.g. Google) places a cookie on the user's computer and organises the advertising in accordance with retargeting target group lists. This cookie is subsequently used to activate re-targeting campaigns ("Interest-related advertising") on other websites. Studies have proven that integrating interest-related advertising is of greater interest for the Internet user than an advert which has no direct relation to the person's interest and previously visited websites.

Who has access to Bytes Technology Group cookie data?

Only Bytes has access to Bytes cookies. Cookies placed by third parties can be accessed by these third parties.

How can you manage your cookie preferences?

Using your browser settings in, for example, Internet Explorer, Safari, Firefox or Chrome, you can set which cookies to accept and which to reject. Where you find these settings depends on which browser you use. Use the "Help" function in your browser to locate the settings you need.

If you choose not to accept certain cookies, you may not be able to use some functions on our website. And opting out of an online advertising network does not mean that you will no longer receive or be subject to online advertising or marketing analysis. It means that the network from which you opted out will no longer deliver ads tailored to your web preferences and browsing patterns.

Does Bytes use web beacons?

As well as using cookies, Bytes sometimes uses web beacons. A web beacon is a tiny graphic image of just one pixel that's delivered to your computer either as part of a web page request or in an HTML email message. Either directly or through service providers, we use these pixels as part of our online advertisements either on our website or on third-party websites to learn whether a user who is being shown an online advertisement also makes a reservation; to track conversion with partner websites and to analyse the traffic patterns of users to optimise the services we bring to you.

Questions, Complaints and Subject Access Requests (SARs)

Any questions or Subject Access Requests (SARs) should be sent to: GDPR@bytes.co.uk.

You have a right to lodge a complaint in the event that you believe that Bytes has not upheld the rights, obligations and responsibilities set out in this Privacy Policy. Please send any complaints to: GDPR@bytes.co.uk.

Review of this Policy

This Policy is regularly reviewed.

SUBJECT ACCESS REQUEST (‘SAR’) PROCEDURE

Introduction

Bytes Software Services (“Bytes”) conducts business-to-business only and does not process large quantities of information about customer individuals (individuals are also known as ‘Data Subjects’). Communication between Bytes and its customers relate to business matters and not about the individual itself, however all individuals (customers, past/present employees/applicants/casual & contracted staff) have the right to submit a Subject Access Request (‘SAR’).

What rights do Data Subjects have?

Data Subjects have the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information (mostly the information provided in privacy notices).
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the information comprising the data; and given details of the source of the data (where this is available).

How do Data Subjects submit requests for their information?

The information Bytes hold is available upon request by contacting GDPR@bytes.co.uk.

Individuals can also request their data is updated and/or deleted at any time, unless Bytes needs to retain it for legitimate business or legal purposes, by submitting a request to this email address.

Responding to Subject Access Requests

Bytes may ask the individual to verify their identity before their request is actioned.

Bytes has the right to ask the individual for enough information to judge whether the person making the request is the individual to whom the personal data relates. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.

Bytes has the right to ask for information that is reasonably needed to find the personal data covered by the request.

If no personal information about the individual is held, they will be informed.

If data processing is outsourced, subject access requests may be sent to the third party to respond.

Bytes’ GDPR Compliance Manager will refer to the Company’s GDPR Data Register to locate all the information held on the individual and liaise with the IT Department plus any other Bytes department and/or Third Parties concerned in order to collate all the information.

Information will be provided within at least one month of receiving the request. Where requests are complex or numerous, Bytes has the right to extend the deadline for providing the information to three months. However, a response to the request explaining why the extension is necessary, will be sent within one month.

Data Access Requests that are manifestly unfounded or excessive can be refused or a charge be made. If a request is refused, the individual will be informed as to why and advised that they have the right to complain to the ICO and to a judicial remedy. The refusal will be made without undue delay and at the latest, within one month.

Information will be provided free of charge.