Dataquest

Your Performance is our priority

Security & Compliance

Dataquest are actively assisting customers across numerous business process areas to help them meet their obligations under GDPR.

Where Dataquest are providing services that include the processing of their intellectual data

We are working with clients to complete Data Asset Risk Treatment Plans, in line with their own Information Security Management System. Where necessary, we also provide controls to mitigate risk and meet the relevant compliances for each data asset type. These controls often include a strategy that encompasses confidentiality, access and integrity as well as reporting and auditing. If you have specific requirements related to data that is processed by Dataquest on behalf of your company, please engage with your account manager to discuss this further.

Where Dataquest provides customers with produces that reside on their premises or within their own network infrastructure

We have published this guide to provide our clients with useful ideas and guidance relating to improving security in the business sectors we operate in. We trust you will also find useful information relating to security services and solutions that are complementary to products we have already supplied. Again for further information please contact your account manager.

For transactional and business communication purposes Dataquest does retain client contact data. For further information about how this is used, please refer to our privacy policy:

https://dataquestuk.com/legal-information/privacy-policy/

Dataquest continues to audit, review and improve our internal Information Security Management System. This encompasses many facets included in our ISO procedural manual relating but not limited to:

- The maintenance of a comprehensive ISMS policy.
- Controls to preserve data Access, Confidentiality and Integrity.
- Auditing, monitoring and reporting of breaches
- Asset registration and risk management.
- Employment procedures including recruitment, screening, on-boarding, training and management of leavers.
- Protection again malicious threats.
- Regulatory and Legislative requirements.
- Adherence to our privacy policy to protect the use of and distribution of customer contact data.

If you have any questions, please direct them to info@dataquestuk.com and by putting “Security enquiry” in the subject line.

Compliance Checklist

Dataquest are proactively helping customers to meet the challenges presented by the arrival of more stringent security and compliance requirements. We start by providing practical advice and configuration to get the best out of an existing infrastructure.

Where regulatory demands necessitate a change in business procedure, Dataquest are providing consultancy for all of our products and services to help drive and facilitate the necessary improvements.

DOCUMENT TECHNOLOGY SOLUTIONS

- Secure Scan
- Secure Print Release
- Auditing
- Robust Hardware & Configuration Services

IT SERVICE AND SUPPORT SOLUTIONS

- Next Generation Firewalls
- Certified Digital Media Destruction
- Endpoint Protection
- Regular System Patching
- Spam Filtering

BUSINESS COMMUNICATION SOLUTIONS

- Mobile Device Management
- Device Utilisation
- Password Management
- Display Privacy Filter
- Mifid II Compliant

MAILING AND POST ROOM SOLUTIONS

- Address Database
- User Training
- Data Encryption

For more information on our security & GDPR compliancy contact: **info@dataquestuk.com**

Secure Scan

Document security demands three things from a policy: confidentiality, integrity and availability. This is never more challenging than dealing with hardcopy paper documents. Paper is by its nature very fragile and easily misplaced. When used exclusively as media for retaining critical records, it means your data is susceptible to theft, misplacement, water, fire, mould, damage and ageing.

By converting hardcopy to an electronic version, it can inherit all the benefits of a secure IT infrastructure. Documents can be fully indexed to bring all relevant information together under an easily searchable interface. In addition, document management enhances compliance by enabling auditing, providing secure sharing, backup and version control.

Dataquest Provide scan workflow, electronic document management and offsite scanning services to digitise records. Our Document Management systems can also integrate with downstream business process and provide a common interface for the storage of emails, PDFs and forms.

Modern scanning workflows can also provide encryption, character recognition and secure connection to Sharepoint, Office 365 and cloud-based applications. This means that users can safely scan, share and work on documents whilst mobile working, without taking the risk of carrying paper documents or utilising easily lost USB storage media

Secure Print Release

Print still represents a fast, cheap and flexible way to share data. The tangible nature of a document still surpasses all the problems of viewing information on devices i.e. screen size, battery power, Wi-Fi connection, spreading of viruses, application conflicts, ease of editing and note taking.

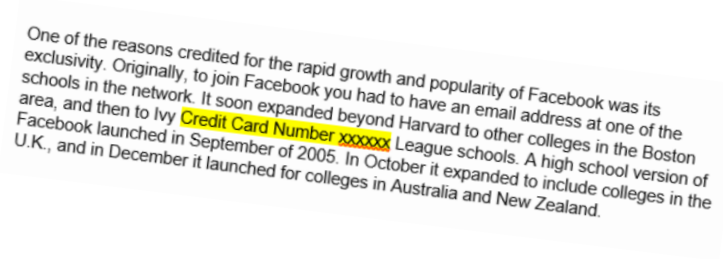
Unless users have the luxury of expensive dedicated personal printers, producing sensitive documents in the workplace can carry its own risks.

From our own figures, 17% of documentsprinted to workgroup printers are never collected. Even documents that do get picked up, are often intercepted and inspected by other employees. Dataquest provides mandatory secure print release solutions. These systems ensures that critical data is only output from the printer once the document owner is authenticated at the printer.

With pull print technology, the document owner can be assured that their print only comes out of the device they are standing at, eliminating rogue print inadvertently sent to the wrong machine or sat behind a long print queue.
Auditing

Auditing

To meet ever more stringent compliance, companies need to proactively audit, monitor and provide evidence that controls are working. Dataquest delivers active print workflows that dynamically scan for information leakage and unwanted data transfer.


One of the reasons credited for the rapid growth and popularity of Facebook was its exclusivity. Originally, to join Facebook you had to have an email address at one of the schools in the network. It soon expanded beyond Harvard to other colleges in the Boston area, and then to Ivy Credit Card Number xxxxxx League schools. A high school version of Facebook launched in September of 2005. In October it expanded to include colleges in the U.K., and in December it launched for colleges in Australia and New Zealand.

Robust Hardware & Configuration Services

Dataquest provides premium networked multifunction devices and printers. These devices provide the newest levels of integrated network security and onboard protection. Dataquest provides our customers with expertise in securing these devices across their network. For security conscious environments we can lock down unnecessary protocols, evoking encryption and provide the quenching of onboard memory to keep your data safe.

Two-Factor Authentication (TFA)

TFA is an extra security measure to verify a user's identity themselves. Dataquest provides TFA as it is an inexpensive measure that is rapidly becoming an industry standard and is being used by most industries including; Law firms, Recruitment, Marketing, Fashion, Technology and Retail to fortify their security.

Vulnerability Assessments

Having antivirus is just the basics of what all organisations should have in practice to keep their systems secure. Vulnerability assessments will find holes in your security. From your servers and other applications. Dataquest runs constant vulnerability assessments so if there are any changes in your servers the will be detected straight away and protected efficiently

Mobile Device Management (MDM)

MDM is essential for organisations to comply GDPR. In brief, all client information has to be protected, and this includes data on mobile devices. Devices that encompass MDM are business mobiles, tablets, laptops and smart watches.Dataquest ensures that the information on the devices is secure by optimising the functionality and security of mobile devices within the organisation, while simultaneously protecting the corporate network

Device Utilisation

Having knowledge of what devices have access to business servers will further help with GDPR and compliance. In the event of a hack, device utilisation allows an expert team to review the data to see what exactly caused the breach, set up future prevention methods and helps to them to secure all other devices that are connected to the same server.

To help with compliance mobile devices should keep personal and business data completely private. The reasons for this is to reduce the risk of being attacked. If you do experience an attack on your personal data and your business data is on the same device then you are more likely to have all data breached. Also, if the data is connected to the business server, this puts all of your organisation's data at serious risk. Dataquest recommends that business devices should have restricted or no access to private emails, social media or other apps.

Display Privacy Filters

Display privacy filters give individuals more autonomy in the workplace by having the user’s laptop or desktop screen visable at a limited viewing angle to passers by. It is a simple but effective way to keep an individual’s data secure. Other benefits of this filter include; being able to work in public areas, reduce glare, computer-related headaches, general scratches and dust.

Address Database

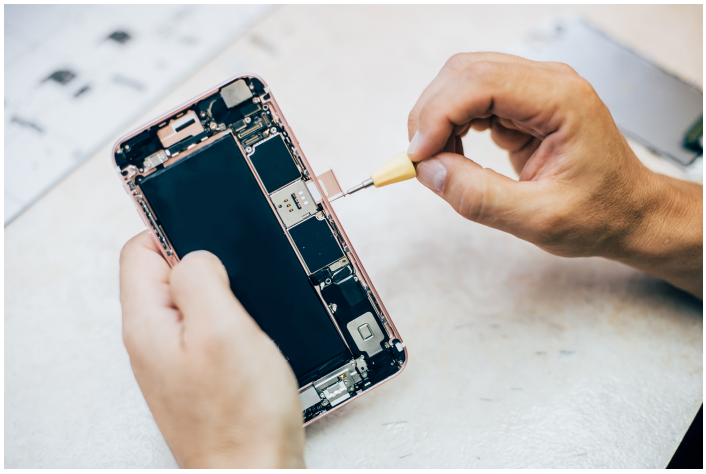
Your mailing and post room data is integral to GDPR compliance. Having names, addresses and other vital information has to be accurate. Maintaining such data is labour intensive and will continually use up precious time. Our Mailmark automated mailing system removes this burden entirely by automatically correcting your database; it also assesses the best postage discount, saving you expenditure and minimising wastage.

On average 22% of address databases are inaccurate, which means a significant proportion of your database will not receive your marketing and other vital communications. An organisation can combat this by using DQ Plus software allows your team to continually review your data across a variety of metrics to feedback what is incorrect giving you a continual improvement cycle to not only comply with GDPR but to improve your message outreach and ROI on marketing campaigns.

Next Generation Firewalls (NGFW)

Our NGFW appliances come with enhanced intrusion prevention, application intelligence, email security, URL filtering, wireless security and virtual private networks. We provide specialist UTM (Unified Threat Management) which fortifies your organisation's cyber security making it more difficult for criminals to exploit.

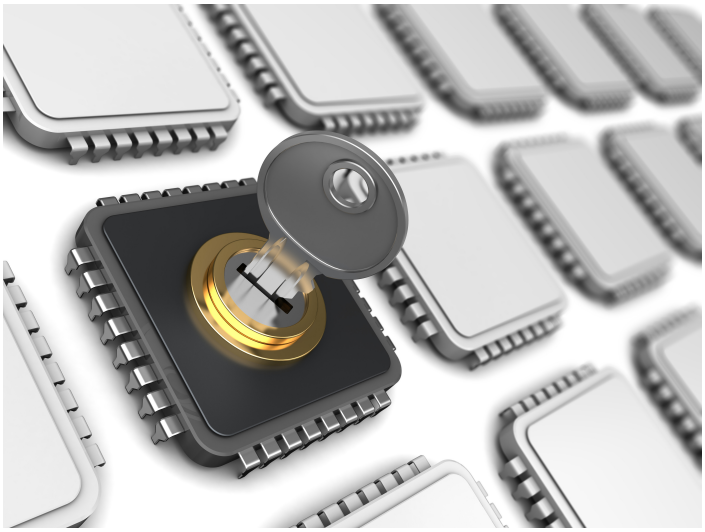
Certified Digital Media Destruction



An almost inconceivable amount of data is stored on external hard drives and USB flash drives. With all of this highly sensitive data saved it would be thought that the information is secure. Unfortunately, this is not the case; data is regularly lost, stolen or thrown away with the information on the devices easily accessible.

Hackers target this unprotected data and sell the information gathered. Many users feel that the data stored on the devices are not sensitive such as emails but this can be highly valuable in the wrong hands and can be used for a variety of crimes including fraud. Dataquest ensures that your data will not be left unprotected and we offer certified digital media destruction for your devices making sure that the data is correctly destroyed so no intruder can access the stored files.

Data Encryption



Data encryption is key to fortifying your data from unwanted sources. Encrypting data is a simple process where an algorithm changes the data into an unreadable format and only allows the intended recipient to access the real information.

Encryption is a powerful security tool; it prevents data breaches, and even if a hacker intercepts the data they are not able to view the information. Having your sensitive data unencrypted is an open invitation to cyber criminals.

There are two main types of data that all organisations should encrypt; this is data on the move and static data. Data on the move is information shared between users, and static data is information that remains in one place such as on a USB stick. Dataquest ensures all moving data in an organisation is secured e.g. encrypted on a VPN (Virtual Private Network), this includes; mobile devices, data traffic between offices and employees that work on the move. Data that remains static is very simple to keep safe, Dataquest realises how vital your data is and, we offer training for your workforce and software to encrypt the data.

Endpoint Protection (Antivirus & Antimalware)

Our Penetration testing assesses your organisation's servers and other internet-connected devices to find vulnerabilities that an attacker could exploit. It is essential to implement penetration testing for two primary reasons regularly:

1. The ways that an organisation's data can be breached is continually evolving, and new vulnerabilities crop up repeatedly.

2. Planned changes to your infrastructure, upgrades & new devices to make retesting frequently essential.

Markets in Financial Instruments Directive (Mifid II)

Mifid II is a security measure put in place to protect investors. The basis of the directive is to record all information that leads to any transaction. The data has to be stored for at least seven years and if the FSA, PCI or DSS requests this information you have to provide it. The investor also has the same level of access but for five years.

Communications using personal devices is stricty prohibited as it is unlikely to be recorded or monitored and investors cannot use personal devices to contact the investor in regards to any transaction as these devices are not monitored or recorded. All recorded information has to be tamper-proof, so it is impossible to edit the material.

Meetings now also require the same level of monitoring. Information that will need to be documented is:

- Time and date of the meeting
- Who arranged the meeting and who is attending
- The premise of the encounter
- What is discussed throughout

Dataquest's phone systems and software are Mifid II compliant. We enable an organisation to monitor all telephone and business mobile calls. The software also allows you to track who makes a call, who answers, the recipient’s general details, time and date. All calls are also encrypted so it cannot be edited or accessed by unauthorised users.

Regular System Patching

System patching involves acquiring, installing testing and code changes to your computer system. Dataquest will regularly check your systems and make sure applications are installed correctly and are up to date. It is essential for not only individuals but for all organisations to patch their systems at the same time to prevent holes in their security and to fortify all users from cyber threats.

Password Management

Passwords are essential for keeping data private; they are low in cost to deploy and have existed for decades. However, being locked out or forgetting a password can be costly. Another problem is when you subscribe to various services you have to create new passwords to remember, and most users will supply the same password for these services or a slight variant. Having the same or similar passwords for these services puts a user at serious risk if one service is breached then all other services are incredibly vulnerable. Dataquest's password manager will securely save your passwords while generating new strong passwords and all the user needs to know is the password for the application.

User Training

Dataquest can assist you in achieving the recognised Cyber Essentials or more stringent Cyber Essentials Plus accreditations.

Dataquest trains your staff to adopt good working practices. Ranging anywhere from spotting infected emails to fake phone calls, Dataquest makes sure that all staff are well trained and ready to recognise breaches and correctly handle them.

Spam Filtering

Staying on top of your emails can be tedious and time-consuming. A high proportion of the workforce receives unnecessary emails which makes it even harder to read and respond to relevant emails. Dataquest has a multitude of spam filters including Fusemail, symantec cloud & mimecast that will significantly reduce these unwarranted emails and they will also filter out most malicious emails.

GDPR will have a considerable impact on marketing emails; users will need to explicitly opt-in to receive this communication and organisations will have to be more targeted with their campaigns to prevent users from unsubscribing.

For more information on our security & GDPR compliancy contact: **info@dataquestuk.com**