



We provide digital and operational security solutions
dealing with resilience and risk

SECR datasheet

How a data security platform can help meet
Streamlined Energy and Carbon Reporting (SECR)



Dataguard ePay
Encrypted Payslips



Dataguard eMail
Encrypted eMail



Dataguard eBox
Encrypted Storage

What does SECR mean for your business?

Q Does your business employ more than 250 employees?

Q Does your business have an annual turnover greater than £36m

Q Does your business have an annual balance sheet greater than £18m

⚠ If you answer 'yes' to two or more of the above questions then SECR applies to you.



The UK Government has announced its plans for the new Streamlined Energy and Carbon Reporting (SECR) regulations to take effect in 2019.

This new mandatory reporting framework will replace the CRC Energy Efficiency Scheme (CRC EES) and extend the scope of the existing Mandatory Carbon Reporting (MCR) regulations for listed companies to all large organisations.

It is designed to streamline and reduce complexity in carbon and energy reporting as well as broaden reporting compliance. This will mean almost a seven-fold increase in the number of companies required to comply with energy and carbon reporting legislation, up from approximately 1,600 now to over 10,000 companies.

Overview

All large quoted and unquoted companies, as defined by the Companies Act 2006, will have to comply with the new energy and carbon reporting framework from April 2019. To reduce the additional burden on reporting companies it is expected that the figures will be published in Annual Reports, alongside financial data.

Companies using 40,000 kWh or less of energy in the 12-month reporting period will be exempt, as will those unquoted companies where 'it is not practical to obtain information'.

Energy in the scope of the new SECR legislation includes all UK electricity, gas, and transport (road, rail, air and shipping) energy use.

How Dataguard can help

Dataguard offers a suite of products built around a highly secure data platform which can help a business migrate from the physical transfer of paper-based confidential data to a digital based system. These products can quickly realise the many environmental and cost gains available without opening up data vulnerabilities or implementation/user difficulties downstream.

Examples of physical transfer of confidential data

Postal/internal mail services

- paper payslips and other confidential employment notices such as P60, P11D, employment contracts

Couriered documents

- standard courier services by motorbike or van or more specialised DX services

Implications of paper based confidential data

If your confidential data is committed to paper and physically sent to the recipient, the environmental consequences are highly significant. From printer consumables to envelopes & packaging, to fuel & pollution from its transportation.

It is natural and understandable for data handlers to be comforted by seeing physical security - opaque envelopes, tamper proof envelopes, strong boxes, safes. But in truth, there are very many vulnerabilities in a paper-based system. Every stage of transfer is a potential vulnerability, from the printer to the desk, from the desk to the mail-out point, from handler to handler, to Reception or mail in. Through internal mail to desk again.

End to end security is a hope, not a guarantee. But digital solutions can also be vulnerable, and the problems have been highlighted frequently for many years. What is needed is a system that provides end-to-end security for confidential data transfer, without sacrificing ease of use, and ease of implementation. Dataguard can now bring this end to end security to your business.

Dataguard paperless solutions

Dataguard ePay



An easy to use digital platform that can bolt on to any payroll system. It securely sends digital payslips and other confidential HR data to

recipients without any of the environmental problems of paper solutions, or the vulnerabilities/user problems of other electronic transmission solutions.

Dataguard eBox



An easy to use method of sharing confidential files amongst a group of users, allowing all the ability to access and amend shared files. This

is facilitated by a platform that provides high levels of security end to end, and allows full audit of group contributions.

Dataguard eMail



End to end security for email communications without the imposition of restrictive operational difficulties for users.

The Dataguard philosophy

Moving from a paper-based system to a digital system requires a high level of confidence in the security of that digital system. Dataguard recognises this and attaches critical importance to data security as an end-to-end process.

As a chain is only as strong as its weakest link, Dataguard ensures that each link of its data process is of equal and high strength. Each stage of the data's 'lifecycle' is rigorously managed so that there is no vulnerable point.



Easy to install. Easy to use

- ✓ Simple to install
- ✓ Simple to manage for both employer and employee
- ✓ Highly secure – AES 256 Encryption
- ✓ Major cost savings from paper solutions
- ✓ Totally scalable -works for any size of organisation
- ✓ Meets latest GDPR/Data Privacy Laws

Organisations using this platform

 International Accountants	 Local Authorities	 World Renowned Hospitals
 Global Technology Companies	 Global Manufacturers	 Housing Associations
 International Footwear Company	 Healthcare Providers	 Multinational Lawyers