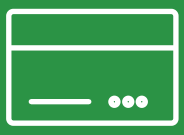
Dataguard™

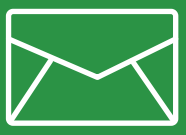
We provide digital and operational security solutions dealing with resilience and risk

eMail datasheet

Secure, encrypted email, easily



Dataguard ePay
Encrypted Payslips



Dataguard eMail
Encrypted eMail

Dataguard eBox
Encrypted Storage

Do you have measures in place to secure your business emails?

- Do you have special measures in place for securing your business email?
- Are you solely relying on strong passwords for your business email accounts?
- Are you using SSL or TLS?
- Are you confident that your data is held safely by your SMTP server, or the email servers of your recipients?
- Do you feel confident that your email processes are secure end to end?

Did you know...

- Email is the electronic equivalent to a postcard. Data is easily viewable at points along the email path.
- Your processes may be in breach of GDPR
- The intellectual property of your business and the confidential data held by key projects may be vulnerable

The components of the Dataguard encrypted email solution

Providing end to end security for your confidential emails is analogous to a chain, in that it will only be as strong as the weakest link. Some solutions will secure some stages of the process, but leave the door open to data breaches at other stages. Other solutions will plug other gaps. But it is essential, if your are serious about your email security, then you require a fully end to end solution.

The Dataguard solution is an end to end solution. One which uses the highest strength protocols and advanced technologies which ensures the message is shared via secured electronic encrypted means and guarantees only the recipient can access the information. It is easy to install and intuitive to use. It offers a system for trusted and binding e-mail communication & digital postal mail.

How it works

Integration with existing email solutions

After registering with Dataguard eMail you can read and write e-mails on the web portal (no software download necessary) or you can use the easy-to-install client software. The software is available as an add-In for Windows (Microsoft Outlook, Lotus Notes, Thunderbird), as a standalone version for Windows, MacOS and Linux as well as an App for iPhone/iPad and Android devices. These options ensure that you can use Dataguard eMail as you prefer.

Step 1: Sending

The Dataguard eMail technology encrypts your e-mail (message text, attachments) and compresses it before it sending it via your and the addressee's e-mail providers as an ordinary e-mail with an encrypted attachment.

This attachment is a regify file with the encrypted contents of your original e-mail. The respective encryption key is transmitted secured and encrypted to the data clearing service via your regify provider.

Step 2: Receiving

In alignment with the data clearing service, the Dataguard eMail provider of the addressee of your e-mail ensures that the recipient is the right person and will transfer the key.

As a result, the recipient can open the Dataguard eMail file and is able to display or store its contents. This is as simple as, for example, opening a pdf file with Acrobat Reader.

Step 3: Confirmation of receipt

When the key is delivered and the Dataguard eMail file opened, the recipient's provider will notify the data clearing service. The data clearing service will notify us who in return, via e-mail, will notify you about delivery of the Dataguard eMail file. Confirmation of receipt is recorded independently of the notification e-mail.

The eMail solution

Easy add-on and use

Dataguard eMail gives you the ability to seamlessly add-on secure digital functionality to your email processes. It allows for intuitive control for all your users

End to end security

You can enjoy high levels of confidence in the confidentiality of your emails.

Send email securely

- Turns normal e-mail into a secure electronic letter
- Works with any e-mail address
- Ensures transparency, creates audit trail through confirmation of receipt
- Can be traced online via the Dataguard eMail transaction register
- Makes ordinary e-mail compliant with the Data Protection Act 2018, GDPR and other legislation
- Integrates into daily business life, e.g. into existing e-mail solutions
- Can be used on mobile devices supporting iOS and Android

Why is eMail so safe?

In order to make sure that your eMail communications are always secured, the emails are encrypted when sent, and the only point where the encryption key meets this encrypted email is at the point where it is received by the recipient.

What is regify®?

The Dataguard eBox service is powered by regify® technology. regify® enables the only network solution for secure and binding e-mail-communication and electronic post. Whereas many vendors narrowly define "secure e-mail" as encrypted e-mail, regify®'s comprehensive solution includes features such as confirmation of receipt and an auditable web-based tracking log of the transactions. regify® elevates ordinary e-mail to the level of a registered electronic letter. Regify®'s secure digital transaction service is globally recognised and trusted . It has been approved by Mastercard to underpin its encryption key technology for its virtual credit cards. Uniquely, these keys are only ever used once and only for each individual transaction.

How does Incert fit in?

Incert Luxumbourg is the equivalent to BACS or UKPAY and is a security clearing house and is used by regify® for managing its Public and Private Encryption Keys. Incert is a public agency under the Luxembourg Ministry of Economy and a recognised centre of expertise. It is based at one of the most secure Tier 4 Data Centres in the world. Tier 4 is the highest level of data storage and is built to be completely fault tolerant and has redundancy for every component. It has an expected uptime of 99.995%. This datacentre is used by regify® as the secure base for its platform

Security standards and algorithms in more detail

A data security process is only as strong as its weakest link. Deploying high level security to only one part of your process, does not, by definition mean your entire process meets that standard. Dataguard is powered by regify® which is based on established standards and proven algorithms which complement each other's strengths right across the data communication process.

regify® uses the following:

SSL encryption
For the connection between the employee and the sender, a SSL connection is used. If you are an authenticated masterEpay member and you are using your identity-file, the complete data transfer will get encrypted in addition to SSL.

AES encryption
The message and attachment (*.rgf file) are encrypted using AES256. A new key is generated for each message. Compared to traditional PKI technology, certificate-based hybrid encryption is not required. As a result, the security of the message does not depend on the security of an RSA key.

RSA encryption
RSA encryption is used for the secure transfer of the message-key to the clearing service.

Dataguard ePay does not have access to the message key. The provider communicates on the basis of an identity-file useing RSA encryption. The information secured by using RSA needs to be secure for just one moment. A secure keylength is not needed by the regify process, as the message-encryption does not rely on RSA keys.

SHA-2 hashcodes
The message integrity is achieved by using SHA hashcodes with a length of 256 bit.

Random number generators, that qualify for cryptography
The random number generator is based on the strict NIST SP 800-90 standard. This is compliant with FIPS PUB 140-2. They are used for generating the key for the regify® message, for

Dataguard Security Ltd
Bloxham Mill | Bloxham | Banbury | Oxfordshire | OX15 4FF
+44 1295 724 101 | dataguard-uk.com