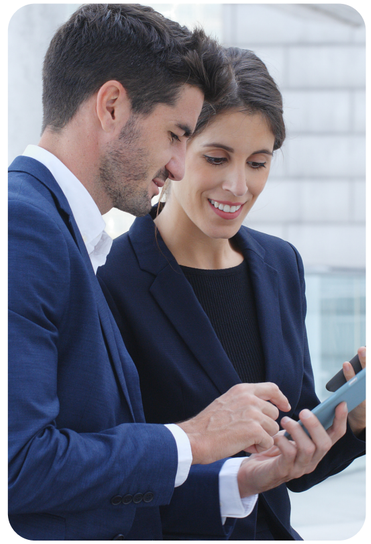
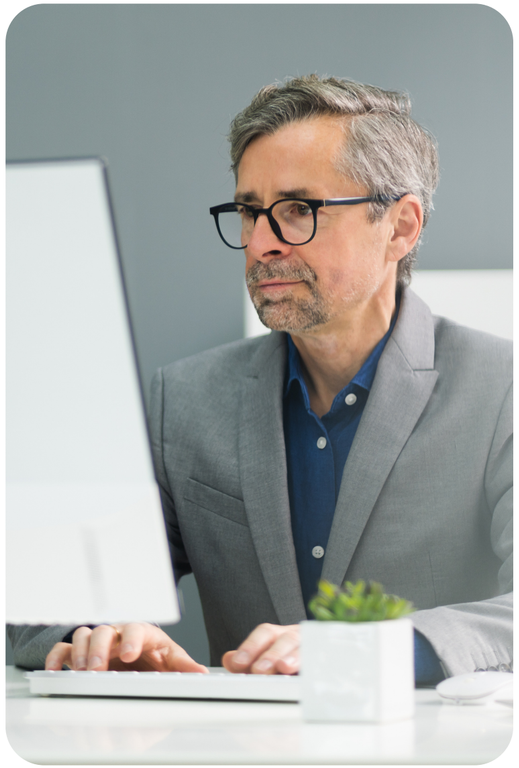
mailock

FINANCIAL SERVICES COMPLIANCE

Compliance Checklist: Financial Services Outbound Email





*

As a financial organisation, compliance is one of the most important considerations for your firm.

Unfortunately, with the ever-changing and complex laws that surround communications, maintaining compliance can present a challenge.

It is a challenge that must be taken on, as failing to adhere to industry regulations can leave your company at risk of reputational damage and hefty fines. One vital area in which compliance must be upheld is within your outbound communications - more specifically, email.

COMPLIANCE CHECKLIST

Compliance for Email

Still utilised as one of the main channels for internal and customer comms, email must be given specific attention when ensuring your company remains compliant.

Although it is a fast and convenient method of transporting documents and other data, email remains unsecured from threats. Ensuring you maintain regulatory standards will help ensure your messages, and the sensitive information within them, remain protected.

We have outlined the main regulations you must be aware of when regularly utilising email, along with the key steps you should take to ensure compliance.

COMPLIANCE CHECKLIST

The General Data Protection Regulation (GDPR)

1.*

GDPR is the European Union’s privacy law, applying to all companies that sell and store personal data about citizens in Europe. There is also a UK specific GDPR, that was slightly changed to accommodate domestic areas of law. The aim was to allow individuals greater control over their information, putting forth ‘rights’ over aspects such as data access and deletion.

Personal data is defined by GDPR as any information relating to an identified or identifiable natural person, including physical, physiological, genetic, mental, economic, cultural and social elements, such as a name, identification number or location data.

With banks and other financial institutions dealing with large quantities of personal data, through processes such as anti-money laundering (AML) know-your-customer (KYC) and fact-finding, it is imperative that GDPR is adhered to at every stage, especially when communicating digitally. To read more on this, you can check out our article on GDPR and email.

2.*

"The previous Data Protection Act, passed a generation ago, failed to account for today's internet and digital technologies, social media and big data. The new Act updates data protection laws in the UK...[and]... provides tools and strengthens rights to allow people to take back control of their personal data."

Elizabeth Denham – Information Commissioner

COMPLIANCE CHECKLIST

The Data Protection Act 2018 (DPA)

The DPA is a UK Act of Parliament which updates data protection laws in the UK and complements the European Union's GDPR. Organisations that are responsible for personal data must follow 'data protection principles', ensuring information is:

- Used fairly and lawfully
- Used for a specific purpose
- Used only when relevant or necessary
- Kept up to date and accurate
- Kept no longer than needed
- Handled in a secure manner, including protecting it against unauthorised access, processing, loss, destruction, or damage.

The final point is an important consideration when ensuring email compliance. As email has little to no inbuilt defences, with any personal data sent within is at risk of being accessed by unwanted third parties and being non-compliant with DPA. This access and loss of data can occur through email interception or human error, such as sending a sensitive email to the wrong recipient.

COMPLIANCE CHECKLIST

3.* The Privacy and Electronic Communications Regulations (PECR)

PECR sits alongside the DPA and UK GDPR, giving people specific privacy rights relating to electronic communications. While GDPR regulates how you store a person's data, PECR governs how organisations are allowed to contact them electronically. PECR includes rules on specific aspects, such as:

- Marketing calls, emails, and texts
- Third-party cookies
- Keeping communications secure
- Customer privacy in terms of traffic and location data, itemised billing, line identification, and directory listings.

It is important to consider PECR if you plan to or are currently sending marketing emails to customers. You cannot send marketing emails to individuals without gaining specific consent first, unless they are a previous or current customer. In this case, you must give the option to 'opt out'.

4.*

"An investment firm shall have sound security mechanisms in place to guarantee the security and authentication of the means of transfer of information, minimise the risk of data corruption and unauthorised access and to prevent information leakage maintaining the confidentiality of the data at all times."

-ESMA, 2021

COMPLIANCE CHECKLIST

Markets in Financial Instruments Directive (MIFID II)

MiFID helps the EU regulate financial markets by creating a singular market for investment services and activities. This ensures there are standardised methods of protection, alongside detailing:

- Conduct of business and organisational requirements
- Authorisation requirements for regulated markets
- Regulatory reporting to avoid market abuse
- Trade transparency for shares

MiFID II also requires that all communications regarding financial transactions are recorded and stored for up to seven years. This includes communications channels such as voice and video calls, instant messaging, social media, SMS, and email.

Communications records must include an audit trail that is clear, easily accessible, and retrievable.

COMPLIANCE CHECKLIST

What Happens if you Don’t Comply?

Besides the damage to an organisation’s reputation, they may also be fined, with UK fines issued by the Information Commissioner’s Office (ICO).

The UK GDPR and DPA can have a maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater – for infringements. The EU GDPR is slightly higher at €20 million (£18 million) or 4% of annual global turnover.

PECR has a maximum figure of £500,000 which can be issued against the organisation itself, or just its directors.

Finally, failure to comply with MIFID II rules could result in fines of up to £5 million or a trade ban.

“You should use encrypted communication channels when transmitting personal data. You should have an encryption policy in place that governs how and when you implement encryption, and you should also train your staff in the use and importance of encryption. When storing or transmitting personal data, you should use encryption and ensure that your encryption solution meets current standards.”

ICO, 2021

COMPLIANCE CHECKLIST

How to Remain Compliant: Encryption

As GDPR and DPA require businesses to safeguard data from unauthorised access, your outbound communications must have a suitable level of protection, especially email. Article 32 of GDPR lists encryption as a suitable method of protecting personal data.

Email encryption is the disguising or scrambling of the contents of your email into code that is unable to be read by human eyes. Content is encrypted and decrypted through the use of keys - strings of randomly generated numbers, with the length directly correlating to their protective strength. You can find out more about encryption here.

Most email providers have a basic level of encryption built-in, however, it doesn’t provide the level of protection necessary to fully comply with regulations. Therefore, organisations should look at implementing an enterprise encryption solution, considering the following things:

- Key size and additional authentication
- Type of encryption - symmetric or asymmetric
- Type of encryption software - does it integration with your infrastructure?
- Scalability and business resilience impact

COMPLIANCE CHECKLIST

How to Remain Compliant: Authentication and Auditing

Another method of ensuring third parties cannot access sensitive information within emails is authentication. When delivering personal data from inbox to inbox, authentication can help businesses to identify recipients before they can read the contents of a message. This eliminates the risk caused by human error and weak passwords.

Multi-factor authentication is considered best practice, providing multiple levels of identity checks before allowing the recipient access. These checks commonly include SMS, Q&A's and biometrics.

As MiFID II legislation requires secure records to be kept, finding an auditing solution that works for email communications is imperative for regulatory compliance. Audit logs can be used to track your messages, checking when emails and attachments were accessed and who by, ensuring only authorised users are reading and downloading the contents.

COMPLIANCE CHECKLIST

How to Remain Compliant: Additional Actions

- Assign a compliance officer - Having an individual in charge of ensuring your organisation adheres to regulations is the best way to guarantee compliance. They can assess your current scope, assist with implementing a compliance strategy and advise what software and processes to put in place.

- Create an internal security policy - Having a company-wide policy that everyone adheres to will help protect assets and demonstrates a strong commitment to security and compliance.

- Educate employees - Compliance solutions are only as strong as the people using them. Teach staff of all levels the fundamentals of regulation and security and how to counteract threats.

Is your firm compliant with industry regulations? Use our checklist to refresh your memory on current legislation and what processes and technology you can implement to adhere to it. Become a data protection leader.

If you need help with securing your email comms, contact us at Beyond Encryption. We empower financial services organisations to communicate digitally, securely, and compliantly. We're protecting communications throughout the financial services industry, connecting advisers, providers, platforms, and third-party services through our secure email solution, Mailock. Get in touch today to see how our team could support you to secure your digital communications.

mailock

Mailock email encryption makes it easy to digitise sensitive communications and maintain full protection and compliance with regulatory standards. Using AES-256 encryption and 2-factor authentication, Mailock empowers businesses to exchange documents with customers, partners, and colleagues using email, without opening their communications up to the risk of a cyber incident.

CONTACT

sales@beyondencryption.com
Beyond Encryption, Gloster Court,
Whittle Avenue, Fareham, PO155SH