



Compliance

“The IDC (International Data Corporation) report that 60% of a business’ critical data is stored via email, so an email archive is vital to store this effectively, securely, and make it easily available to search for”

Mike Kenyon

“The industry in which we operate is compliance driven and we simply could not take any chances... We need complete confidence in the compliance aspect of inbound and outbound emails”

**Leon Sale,
IT Manager at Baker
Tilly**

“From a personal point of view I don’t have to worry so much about managing my emails, which is great”

**Employee, North
Warwickshire
Borough Council**

“In terms of searching, Cryoserver has saved hours of people’s time”

**Martin Vogwell,
IT infrastructure
manager,**

How long should your business keep its emails?

Every business needs to understand the Data Protection Act (DPA, 1998). It aims to protect the privacy and protection of all personal data collected for or about citizens in the UK. It states that data should be kept for ‘no longer than is necessary’. So, what does this mean for email retention? Well, that depends. Different data requires different retention times. Whilst we can’t include every single piece of legislation, here are just a few of the regulations for your business to consider:

Limitation Act 1980

These regulations place a time limit on starting legal proceedings for civil actions. The act allows businesses a guideline for how long to keep certain information which may be of use in future if a court case arises. For example, employment tribunal court claims are possible for up to six years after employment is terminated. Therefore, personnel information should be kept for six years after an employee’s departure from a business.

Companies Act (1985/2006)

These regulations place a time limit on starting legal proceedings for civil actions. The act allows businesses a guideline for how long to keep certain information which may be of use in future if a court case arises. For example, employment tribunal court claims are possible for up to six years after employment is terminated. Therefore, personnel information should be kept for six years after an employee’s departure from a business.

“We use [Cryoserver] when we have Subject Access Requests (SAR) or Freedom of Information (FOI) requests... Cryoserver helps us to carry out searches quickly and securely”

Vincenzo Ardilio
Guildford Borough
Council

IMPORTANT TO KNOW

Are you in the healthcare / pharmaceutical industry? Or in one where employees have health & safety risks? Regulations on data retention are more stringent for such industries. Whatever your business, it has 20 working days to respond to a Freedom of Information (Fol) request, and 40 calendar days to a Subject Access Request (SAR). Despite leaving the EU, UK businesses must still comply with EU GDPR and protect personal data. Failure to do this can incur fines of up to €20m or 4% of a company's global revenue.

Working Time Regulations

These laws govern maximum working hours, including maximum weekly working time limits, night work limits, and health assessments for night work. Any records of communication about these regulations are to be held for two years.

Statutory Maternity/Sick Pay Regulations

Employers must keep maternity pay records and certificates, along with sickness records, for three years after the end of the tax year to which they relate. That is, the year in which the maternity pay period ends; or, for sick pay, three years after the tax year to which it relates.

Financial Services Authority

In the UK, the Financial Services Authority (FSA) regulates financial service providers. The FSA's regulations require all financial institutions to store all business emails, sent and received, for up to six years, and some emails indefinitely, so that cases can be reviewed.

Freedom of Information Act (2006)

The aim of this act was to create a more open government based on mutual trust. It provides public access to information held by public authorities. Anyone is entitled to make a Freedom of Information (Fol) request to public bodies, or a Subject Access Request (SAR) to a business, in which they can gain access to information recorded about themselves. This information can be both official and unofficial (i.e. drafts, emails, notes, CCTV, phone recordings) as well as information not created by the company itself, i.e. letters from members of the public.

Compliance with Cryoserver

Ever since we started, our email archiving has always had compliance at its heart. Whatever your industry's regulatory requirements, you can be confident you're covered with Cryoserver.

We are proud to work across many sectors with industry leaders and highly respected clients. These include blue chips, local governments, charities, financial services and law firms.

We are one of the pioneers of email archiving. With our many years of experience, investment and development, Cryoserver technologies deliver highly complex and ultra-secure systems with simple, easy-to-use interfaces. Everyone can benefit from our expert archiving solutions.

Expertly Simple Email Archiving and Compliance