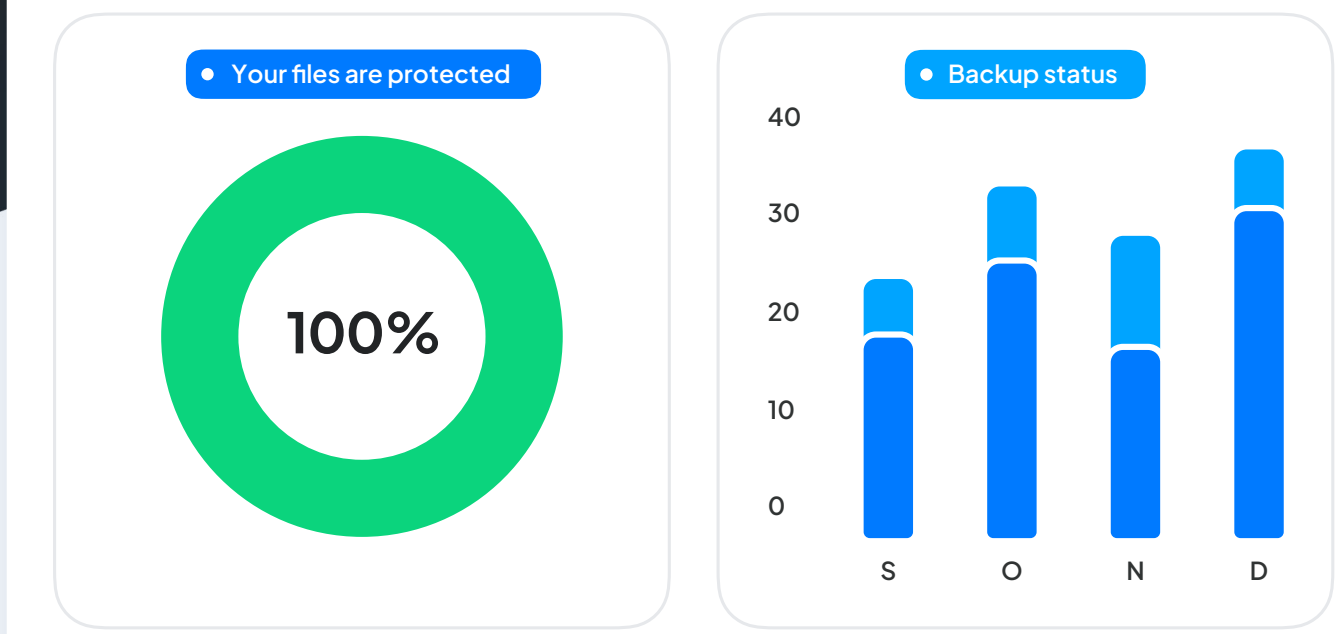
BACKUPVAULT

Legally backed up: The art of effective and compliant data backup for insurance companies



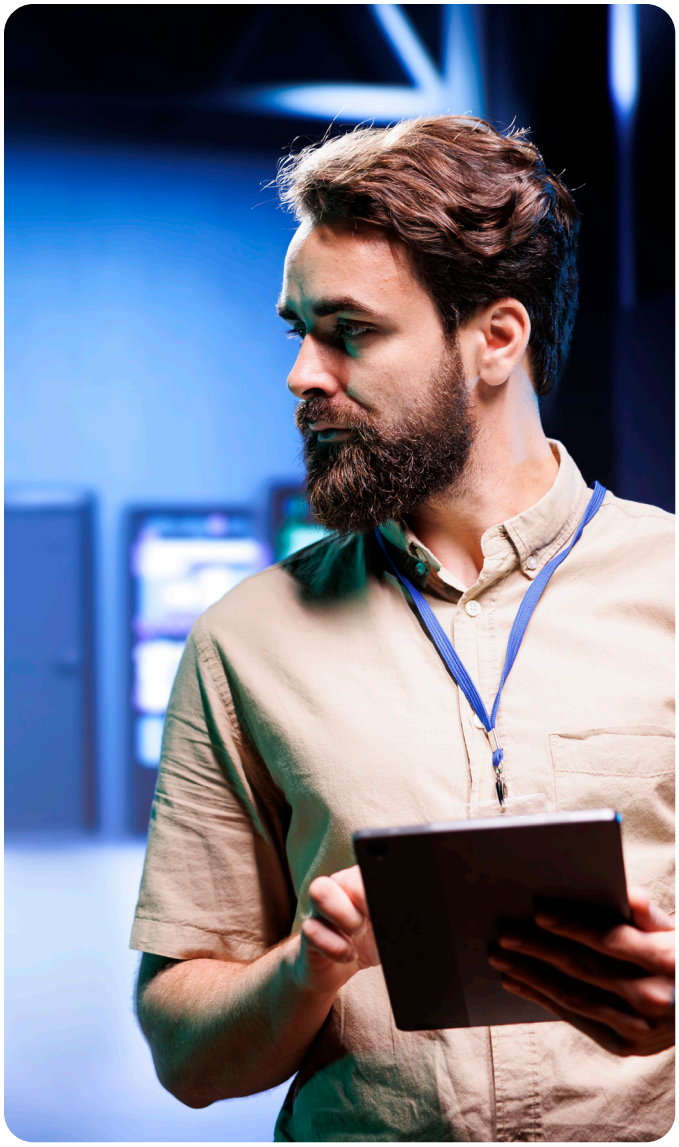
In today's rapidly evolving digital landscape, a growing number of industries rely on data to streamline operations and stay competitive. However, as technology advances, new challenges arise that demand innovative solutions and adaptable strategies to ensure continued success.

Given the sensitive nature of the client and case information insurance companies handle daily, an effective data backup strategy is now essential for not just regulatory compliance but also for:

- **Maintaining business continuity**
- **Safeguarding company reputation**
- **Minimising operational risk**
- **Ensuring data security and privacy**

In this eBook, we'll be exploring the topic of data backup within the insurance industry and examining the type of data that needs to be legally backed up, as well as the best practices for implementing a data backup strategy that offers more than just legal compliance benefits.

Let's get started!



The importance of data backup in the insurance industry

Whether it's customer records, claims histories, financial transactions, or policy details, insurance companies lean heavily on accurate and accessible data. With this in mind, it's easy to see how data loss could significantly impact your workflow.

Leading to financial setbacks, operational bottlenecks, and potential damage to your reputation — ineffective management of your data can have severe consequences for your organisation.

Due to the sensitive nature of the data being handled and stored by insurance companies, it's also important to consider the potentially damaging emotional impact of an ineffective data backup strategy on clients and stakeholders.

Particularly for those involved in complex legal cases and sensitive claims, the legal implications of data loss are just one of the many challenges facing insurance companies.

What are the main causes of data loss for insurance companies?

For insurance companies, data loss can occur for several reasons. While some instances fall outside the control of business owners and employees, others are a direct result of ineffective or non-compliant data protection policies. Some of the main causes of data loss for insurance companies include:

- **Human error**
- **Targeted cyber or phishing attacks**
- **Unforeseen disasters, e.g. on-site fire or flooding**
- **Hardware malfunction**

Navigating the legal landscape of data backup

Building an effective & legally compliant data backup strategy

As a reputable insurance company, a data breach can cast a significant shadow over your company's image.

As mentioned, in addition to compliance issues, data loss or misuse can damage your brand image and erode customer confidence overnight — making it difficult to maintain relationships and implement growth plans.

This is why when it comes to safeguarding sensitive client and case information, a well-thought-out data backup strategy is not just a sensible choice; it's a critical one!

Wondering where to start? Our team of experts is here to help.

Note: While this eBook provides insightful perspectives, it's important to clarify that it is not intended as a substitute for professional legal advice.

Research your obligations

01

Data backup regulations within the insurance sector are far from uniform; they can vary depending on geographical boundaries, local data protection laws, and industry-specific mandates.

This is why before building a data backup strategy for your insurance company, it's vital to research your obligations depending on your unique business model and the type of clients you serve.

We'll now discuss a small selection of the regulations and legal guidelines you need to be aware of as an insurance company in the UK.

General Data Protection Regulation (GDPR)

Despite being one of the most well-known data protection laws in Europe, GDPR can also be one of the trickiest regulations to satisfy. Just some of the key principles of GDPR include:

- **Lawfulness, fairness, and transparency:** Data processing must satisfy all legal requirements and be managed fairly and transparently.
- **Purpose limitation:** Data should be collected only for explicit, legitimate purposes.
- **Data minimisation:** Data should be gathered only when necessary and with clear intent.
- **Accuracy and data quality:** Collected data should remain accurate and up-to-date.
- **Storage limitation:** Data should be stored for the shortest necessary time.
- **Consent consideration:** Evaluate whether consent is necessary from the individuals whose data you seek to collect.
- **Data protection officer:** Determine if appointing a data protection officer is necessary for your organisation.
- **Integrity and confidentiality:** Measures should be put in place to ensure data is secure from unauthorised access.
- **Accountability and compliance measures:** Organisations must demonstrate full accountability for their management of data and associated risks.

When it comes to building an effective and compliant data backup strategy, GDPR should be one of your first ports of call to ensure your strategy is on the right track.

Data retention policies and timelines

Even though UK GDPR does not dictate how long you can retain personal data, it is up to each individual insurance company to justify the need for withholding data and the length of time it is being retained. To satisfy this requirement, your data backup strategy should take into consideration:

- The type of data being backed up and stored
- How appropriate your management processes are for specific data
- The permissions granted by the person the data is relevant to

UK insurance regulations & FCA directives

As a UK insurance company, conforming to regulations set out by the Financial Conduct Authority's (FCA) is essential for maintaining legal compliance. The FCA's mission is to ensure the integrity, fairness, and transparency of financial markets and protect consumers' interests. Mandates set by the FCA cover a broad spectrum of operations within the insurance industry, some of which include:

- **Customer treatment:** Ensuring fair treatment of customers, clear communication, and transparent disclosure of terms and conditions to build trust and maintain ethical business practices.
- **Risk management:** Implementing risk management strategies to safeguard both company assets and customer interests, reducing potential financial instability.
- **Financial stability:** Meeting capital and liquidity requirements to ensure the financial stability of your insurance company (minimising the risk of insolvency).
- **Market conduct:** Conducting business with integrity, preventing market abuse, and fostering healthy competition within the insurance market.
- **Claims handling:** Adhering to efficient and ethical claims handling procedures, ensuring timely payouts while preventing fraudulent activities.

As part of your data backup strategy, it's important to keep up to date with the latest announcements from the FCA. This not only helps ensure your strategy is actively compliant, but it also acts as a good guideline for the direction in which industry standards are moving.

Solvency II guidelines

EU-based insurers must also align operations with Solvency II's data management principles. Solvency II sets out to unify the EU insurance market and enhance consumer protection.

As part of Solvency II, insurance companies should be aware of the following three "pillars" when building an effective and compliant data management strategy:

- **Pillar 1:** This pillar involves calculating capital requirements based on insurance liabilities and risk assessments. This ensures insurers have sufficient resources to cover potential losses.
- **Pillar 2:** Pillar 2 is essentially a supervisory review process of internal control systems to determine if risks can be managed appropriately.
- **Pillar 3:** Based on the promotion of market discipline, pillar 3 dictates that insurers should adhere to reporting and transparency requirements. This makes it easier for stakeholders to assess an insurer's financial health.

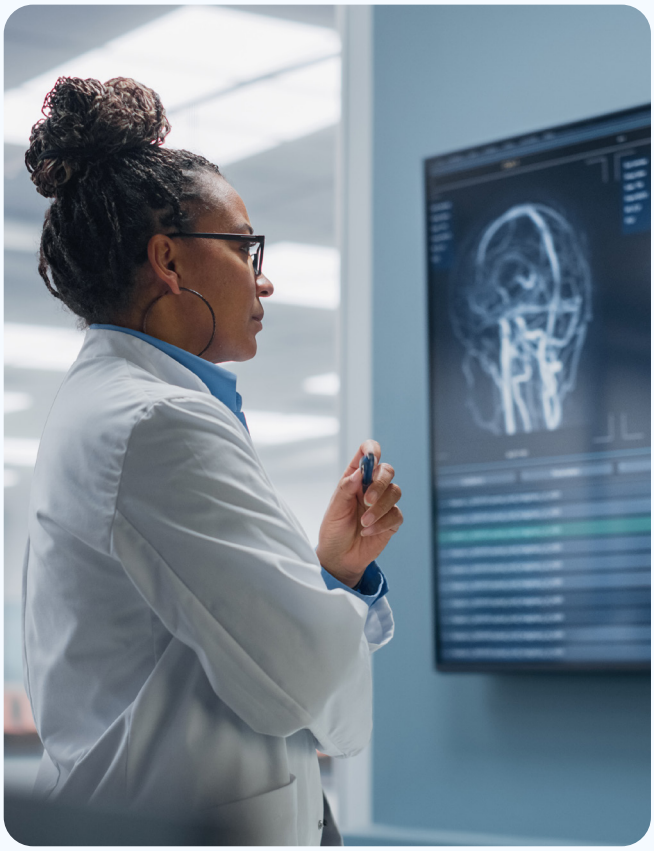
Handle all data with care — but prioritise personal & sensitive data

02

The insurance sector handles a diverse range of sensitive data. Ensuring the preservation of this data is vital for not only legal purposes, it's also essential for nurturing trust among policyholders.

While a comprehensive data protection framework is recommended for long-term success, a good starting point is to focus your resources on protecting your insurance company legally. So, as an insurance company, what type of data and regulations should you be prioritising as part of your data backup strategy?

As a baseline, insurance companies should aim to safeguard and manage all data effectively and compliantly. However, a particular focus should be placed on:



- Customer records & policy details
- Claims & case information
- Medical records
- Financial transactions & history
- Personal identifiers & communication records

Keep up-to-date with the latest in cyber security

03

Cyberattacks are becoming increasingly sophisticated, and new vulnerabilities are being discovered regularly.

By keeping up-to-date with cyber security news and developments, you can gain valuable insights into emerging threats, vulnerabilities, and best practices for safeguarding your insurance company's sensitive data. To do this, we recommend:

- Subscribing to reputable cybersecurity news sources, e.g. the National Cyber Security Center (NCSC.GOV.UK)
- Participating in industry forums
- Engaging in relevant webinars
- Availing of free trials to test out new data protection measures
- Following the work of cyber security figures

Partner with leading data protection experts

04

Crafting an effective backup strategy requires a multi-faceted approach, something many insurance companies find overwhelming and often lack expertise in. This is where partnering with established data protection experts can make a big difference.

From Cloud backup service providers to security awareness trainers, these experts specialise in understanding the intricacies of data security, compliance regulations, and the evolving cyber threat landscape.

By collaborating with data protection experts, your insurance company can offload the complex task of data backup and security, allowing you to focus on your core operations with confidence.

When choosing a data protection partner, consider the following:

- **Tailored solutions:** Each insurance company's needs are unique. Partner with experts who understand this and can tailor their solutions to match your company's size, operations, and data handling practices.
- **Comprehensive services:** Your chosen partner should offer a range of services, including data backup, encryption, regular security assessments, and incident response planning.
- **Reputation and experience:** Look for a partner with a proven track record of assisting businesses in the insurance sector.
- **Up-to-date knowledge:** Data protection is an ever-evolving field. Your partner should stay updated with the latest regulations, technologies, and best practices to provide you with the most effective solutions.
- **24/7 support:** Cyber threats can emerge at any time. Ensure your partner provides round-the-clock support to assist you in case of emergencies or unexpected security incidents.

Choose cloud backup for the ultimate piece of mind

05

Even though on-site data backup is better than no backup at all, the benefits of Cloud backup have become increasingly apparent in recent years.

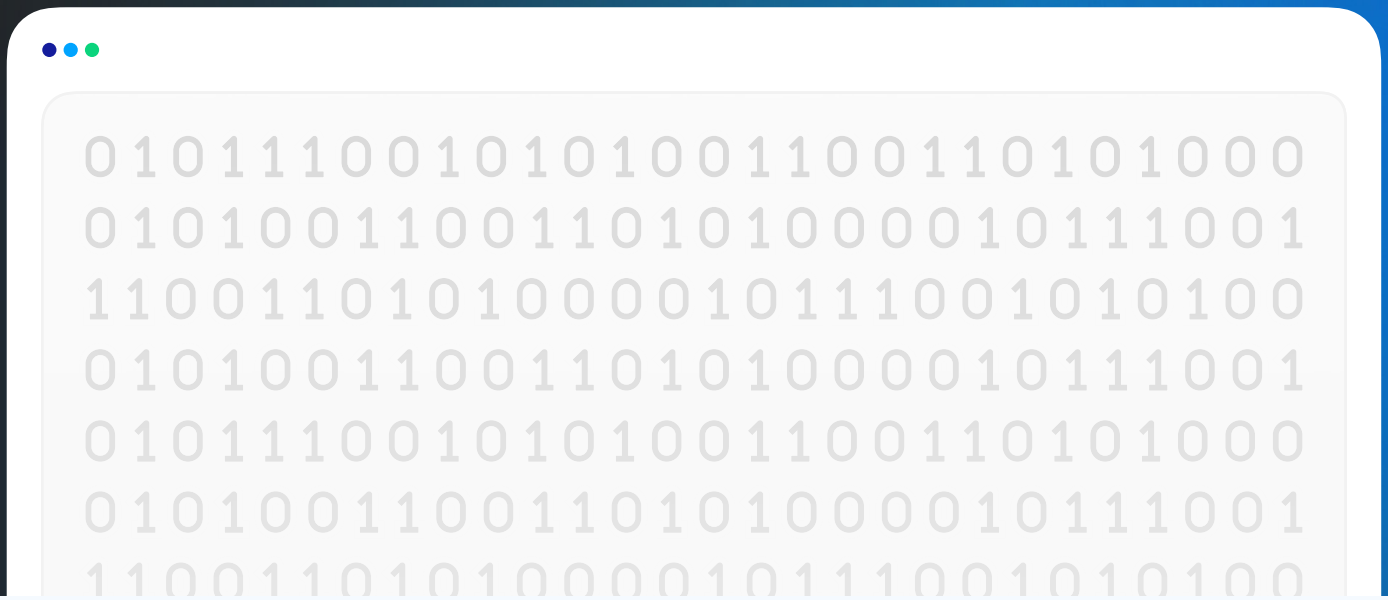
Cloud backup eliminates the risks associated with physical storage systems while ensuring seamless data recovery in case of unexpected events. Just some of the benefits of reliable Cloud backup services include:

- Secure data encryption for enhanced protection
- Automated backups that reduce the potential for human error
- Remote accessibility for data recovery from anywhere
- Scalability to accommodate growing data needs
- Regular updates and maintenance of security protocols
- Cost-effectiveness compared to maintaining on-site infrastructure

With service providers such as BackupVault offering additional benefits such as UK data centres and 24/7 customer support, kick-starting your data backup strategy has never been easier.

To learn more about BackupVault's services, start your 14-Day Cloud Backup trial today or get in touch with a member of our expert team.

Free trial



BACKUPVAULT

backup@backupvault.co.uk

020 3397 5159

Wilson House, Lorne Park Road
Bournemouth, Dorset, BH1 1JN