

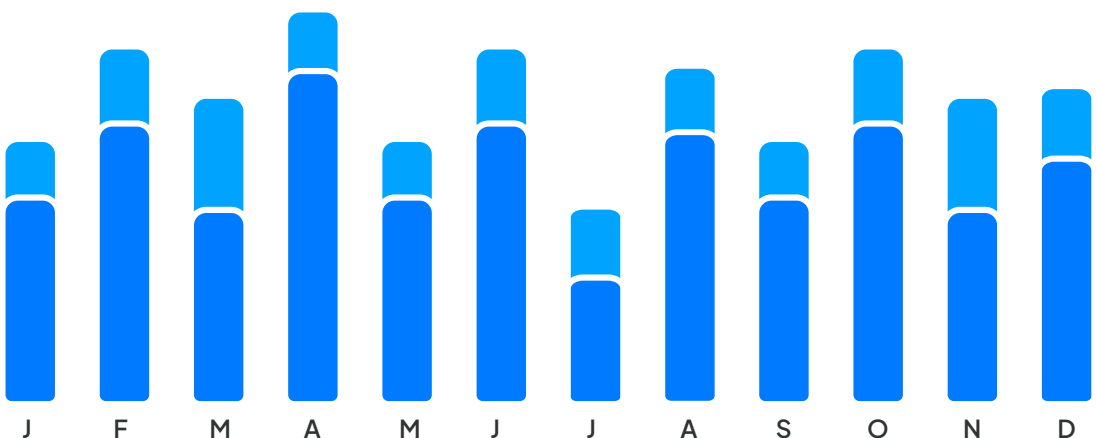


Legal obligations: Essential data backup requirements for agency owners



• Backup status

40
30
20
10
0





As an agency owner, you manage sensitive client information, spanning marketing strategies, customer insights, and financial data.

However, data loss can happen for various reasons, such as hardware failures, cyberattacks, human errors, and more.

Ensuring the security of your confidential data is not only crucial for upholding your customers' trust and maintaining your agency's reputation; it's essential for regulatory compliance as you have a legal responsibility to safeguard sensitive information.

Fortunately, having a reliable backup system can help you mitigate legal risks

and allow you to maintain the integrity, confidentiality, and accessibility of critical agency data.

In this guide, we'll explore the ins and outs of the sensitive information you must back up to comply with data protection laws.

We'll also take a look at some of the most common mistakes agencies make while backing up their data and how you can avoid these common pitfalls to ensure the continued success of your organisation.

What is data backup, and why is it important for agency owners?

Data backup involves creating copies of important digital information and storing them in a separate location from the original data, whether locally, in the cloud or in another remote location. This practice is crucial because it provides a safety net

if the original data is lost, corrupted, or compromised due to a data breach or other unforeseen circumstances.

For agency owners, data backup is important because it:

- ✓ **Safeguards sensitive data:** Backups ensure sensitive data can be restored in case of loss or compromise.
- ✓ **Ensures compliance:** Backup systems help meet legal and regulatory data protection requirements.
- ✓ **Builds client trust:** Protecting client data is crucial for trust. Backups show commitment to data security.
- ✓ **Preserves intellectual property:** Backups safeguard valuable creative assets and intellectual property.
- ✓ **Maintains operations:** Backups enable quick recovery from disruptions like cyberattacks or hardware failures, minimising downtime.
- ✓ **Saves costs:** Data recovery can be expensive. Regular backups reduce recovery expenses.



What data is your agency required to back up?

Your agency is responsible for safeguarding a wide array of crucial data to guarantee security, accessibility, and integrity.

Conforming to data regulations such as General Data Protection Regulation (GDPR), The European Data Protection Board (EDPB), and The Data Protection Act 2018 is essential for complying with UK data laws.

The types of data requiring backup can vary depending on your agency's activities, industry, and regulatory obligations.

While the exact details may differ, here are some common categories of data that agencies are typically required to back up to meet privacy and data protection regulations:

01

Client information

Safeguarding sensitive client and personal data collected by your agency is paramount. This includes contact details, contracts, and communication records. Maintaining backups on each data subject ensures that client trust remains intact and their confidential information is protected.

02

Financial data

The financial backbone of your agency must be secured. You're required to backup financial records such as invoices, payment information, transaction logs, payroll data, and essential tax documents. This ensures smooth financial operations and helps with auditing and regulatory compliance.



03

Creative assets

For agencies involved in design, media production, or creative content, it's crucial to preserve creative assets.

This includes design files, graphics, videos, advertising materials, and any intellectual property your agency generates.

04

Marketing Strategies

As part of data protection rules, you must also back up marketing plans, campaign strategies, and related documents. These represent the heart of your agency's campaigns and initiatives, and their preservation is vital for future reference and planning.

05

Website and content

If your agency manages websites, blogs, or other online content, ensure comprehensive backups of both website files and databases. This precaution ensures that your online presence can be swiftly restored in case of website issues or cyber incidents.

06

Employee records

Your agency's workforce is a valuable asset. Backing up employee data, contracts, performance evaluations, and other HR-related documents maintains a comprehensive record of your team's journey and is essential for legal compliance.



07

Communication records

Your agency's communications are rich in critical decisions, instructions, and insights. Backing up emails, chat logs, and other communication records is essential to keep a record of key discussions and actions.

08

Software and application configurations

Preserve backups of software settings, configurations, and licences. This ensures that your agency's tools and software can be quickly restored to operational status in case of system failures.

09

Client projects

Back up project files, progress reports, and any communication related to ongoing or completed projects. This safeguards the hard work put into client projects and ensures that project-related information is always accessible.

10

Intellectual property

If your agency holds intellectual property such as trademarks, copyrights, or patents, ensure these assets are backed up. This guarantees the protection of your creative and innovative endeavours.

Common data backup mistakes to avoid

By learning from common data backup errors made by agency owners, you can take proactive measures to safeguard your agency's sensitive information and ensure you don't make the same mistakes.

- ✓ **Infrequent backups:** Neglecting regular data backups can lead to data loss if files are accidentally deleted or something goes wrong. Consistent backups ensure the latest versions are securely stored.
- ✓ **Inadequate storage space:** Insufficient storage planning can result in incomplete backups and lost information. Adequate space should be planned for as data grows.
- ✓ **Security oversight:** Failing to encrypt backup data risks confidentiality during transfers or storage. Encryption protocols and security awareness training are vital.
- ✓ **Not testing backups:** Failing to test backups regularly can create a false sense of security. Regular testing guarantees correct and swift data recovery during critical situations.
- ✓ **Lack of disaster recovery plan:** Without a clear disaster recovery strategy, agencies are unprepared for data loss incidents and disruptions. A well-defined plan is essential for timely recovery.
- ✓ **Neglecting important data:** Treating all data equally during backups might lead to overlooking crucial information. Proper prioritisation ensures vital datasets receive proper protection.
- ✓ **Storing backups together:** Keeping backups near original files poses risks in case of disasters or breaches. Safeguarding involves storing backups in different secure locations.
- ✓ **Ignoring data versioning:** Lack of multiple backup versions complicates recovery from changes or corruption. Data versioning maintains historical file versions.
- ✓ **Manual vs. automatic backups:** Manual backups can lead to errors and inefficiencies. Automated backups streamline operations, ensuring reliable and timely protection.
- ✓ **Neglecting backup monitoring:** Failing to monitor backups can lead to unnoticed failures. Monitoring tools prevent issues from going unnoticed.

A robust backup strategy is essential for agency functioning and data protection. Awareness of these ten common mistakes equips you with practical solutions to avoid them effectively.

Key takeaway

In the dynamic world of agency ownership, safeguarding sensitive data isn't only about trust and reputation—it's a legal mandate. Financial data, client information, creative assets, and communications are among the critical pieces that require secure backups for legal compliance.

Fulfilling these obligations isn't always smooth sailing. Agencies often stumble due to common data backup errors. By following the insights into these pitfalls outlined in these eBooks, you can apply practical solutions to steer clear of them.



Protect your agency's data with BackupVault!

Take decisive action and fortify your agency's vital information using BackupVault. Our advanced solution offers automated cloud backup and robust data protection against ransomware, insider breaches, hacking attempts, and beyond.

With BackupVault, you can securely store and restore data seamlessly, whether you're using Microsoft 365, Google Workspace, SQL databases, Azure, servers, desktops, or NAS devices.

Our comprehensive backup process is designed to meet the diverse needs of modern agencies, providing peace of mind thanks to appropriate security features for your critical data.

Embark on a 14-day free trial and unlock the advantages of dependable backup storage and effortless data recovery with BackupVault.

✓ Free trial

Disclaimer: Please note that the information and data protection principles provided are not legal advice, and the specific requirements for data backup may vary depending on your jurisdiction. It is essential to consult with legal professionals to ensure compliance with relevant regulations or for further information on a specific data protection law.



✉ backup@backupvault.co.uk

☎ 020 3397 5159

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

