DATA SUPPORT HUB

The Top 6 GDPR Mistakes

How to Prevent the Top 6 Costly Mistakes

Data Support Hub, July 2024

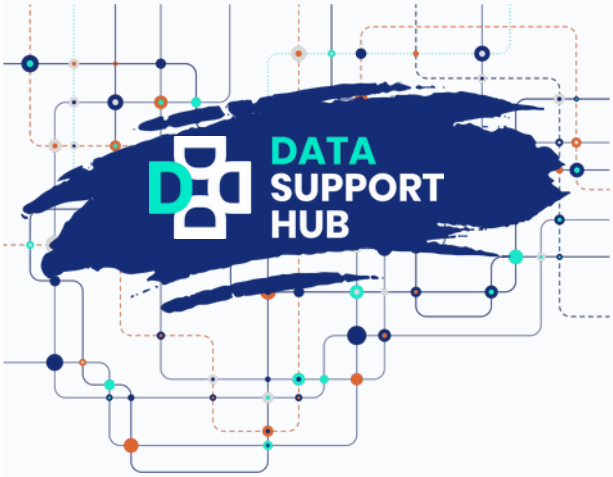
datasupporthub.com contact@datasupporthub.com

DATA SUPPORT HUB

Introduction

Stay GDPR Compliant: How to Prevent the Top 6 Costly Mistakes

The General Data Protection Regulation (GDPR), implemented in May 2018, revolutionised the landscape of data privacy across the European Union and beyond. Despite its far-reaching implications, many businesses remain uncertain about their compliance status. The complexity and nuances of the current UK GDPR can be daunting, and non-compliance can result in hefty fines and irreparable damage to a company's reputation. However, understanding and avoiding common pitfalls can significantly reduce these risks. This white paper explores the top six GDPR mistakes businesses often make and provides practical steps to overcome them.



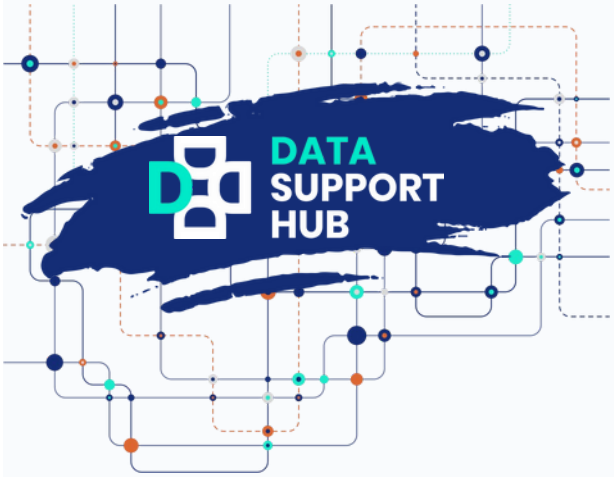
1 Still Operating Under EU GDPR

The Pitfall

Some organisations are still adhering to the EU GDPR as implemented in 2018, mistakenly believing it suffices for current data protection needs. When the GDPR was implemented in 2018, a new UK Data Protection Act (DPA) took effect at the same time to describe rules specific to the UK.
Following the Brexit transition period, the UK GDPR superseded the EU regulation in 2020. The UK GDPR sits alongside an amended version of the DPA 2018.

The Solution

Businesses must update their data protection frameworks to align with UK GDPR and the DPA 2018. This includes conducting a comprehensive review personal data held within the business and ensuring all requirements for use or transfer are met. Implementing an ongoing data protection compliance program is crucial, involving regular audits, data mapping, and reviews.



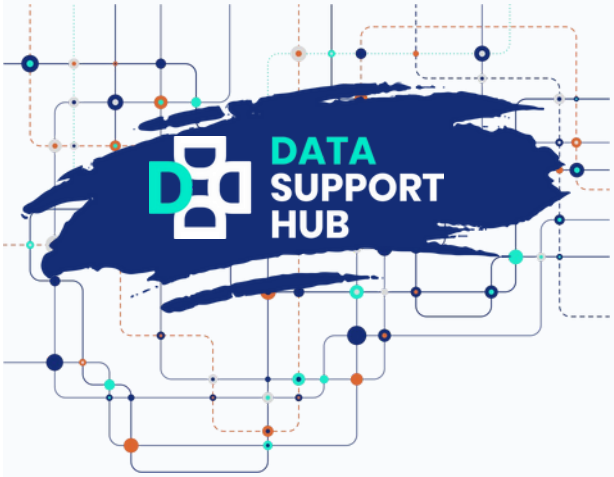
2 Only Updating Privacy Policy

The Pitfall

Updating the privacy policy alone is insufficient for UK GDPR compliance. While a transparent privacy policy is essential, the UK GDPR encompasses a wide range of obligations that go beyond documentation. Once all these requirements are met, the privacy policy can be written to reflect the current use of personal data within an organisation.

The Solution

Compliance requires a holistic approach. Businesses must implement robust data protection measures, including proper security measures, ensuring data accuracy, and providing mechanisms for individuals to exercise their rights (e.g., right to access, right to be forgotten). Regular training for staff and appointing a Data Protection Officer (DPO) where necessary are also key steps.



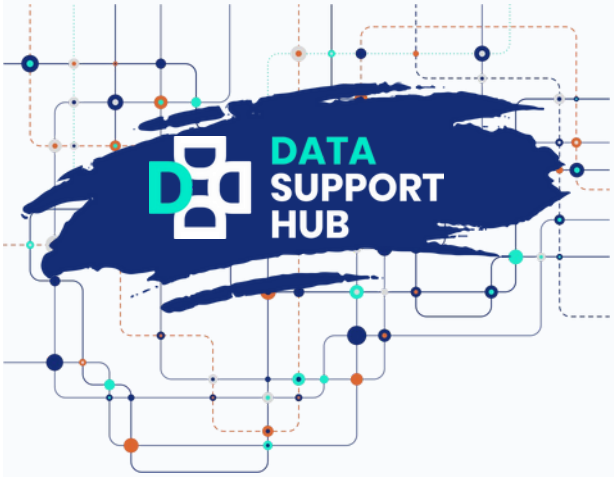
3 Ignoring Retention Periods

The Pitfall

Failing to establish and adhere to data retention periods can lead to non-compliance. GDPR mandates that personal data should only be kept for as long as necessary for the purposes for which it was collected. It is important to know what personal data is held, why it is held and how it should be managed.

The Solution

Implement clear data retention policies that specify the duration for which different types of data will be retained. Regularly review and securely dispose of data that is no longer needed. It is important to keep a record of reviews and data destruction.



4 Sending Unprotected Personal Data via Email

The Pitfall

Transmitting personal data through unencrypted emails exposes it to unauthorised access and data breaches, violating GDPR's data security requirements. The possibility of human error, such as sending data to the wrong email address, greatly increases this risk.

The Solution

Ideally, secure file transfer methods should be used to transfer personal data to mitigate any risk. In cases when this may not be possible, encrypting emails containing personal data protects against interception and unauthorised access. Training for all staff, repeated regularly, will ensure that they are aware of the importance of data security.

5 Using Children's Data Inappropriately

The Pitfall

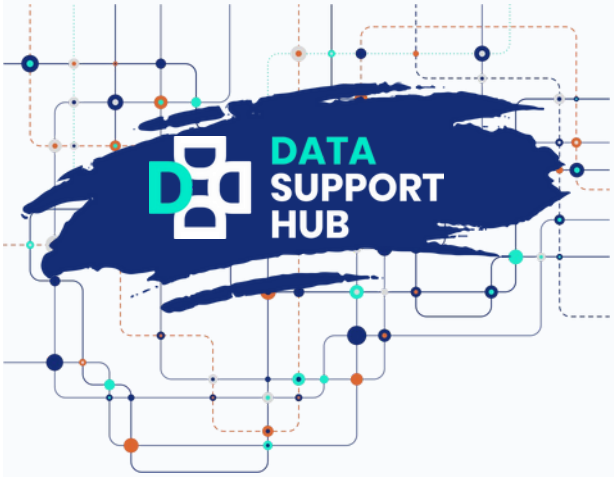
UK data protection law mandates that organisations collecting personal data while offering online services to children under 13 must first obtain consent from a parent or guardian. TikTok fell short in this area, neglecting to ensure it had the necessary consent, even though it was likely aware that children under 13 were active on its platform. Moreover, TikTok did not implement sufficient measures to identify and remove underage users.

The Solution

When processing children's data, you must consider how to ensure the age of the child is verified. You must consider the risks to children that arise from your platform or service and select an approach that is appropriate and proportionate to the risk.

"An estimated one million under 13s were inappropriately granted access to the platform, with TikTok collecting and using their personal data. That means that their data may have been used to track them and profile them, potentially delivering harmful, inappropriate content at their very next scroll. TikTok should have known better. TikTok should have done better. Our £12.7m fine reflects the serious impact their failures may have had. They did not do enough to check who was using their platform or take sufficient action to remove the underage children that were using their platform."

- John Edwards, UK Information Commissioner



6 Not Training Staff

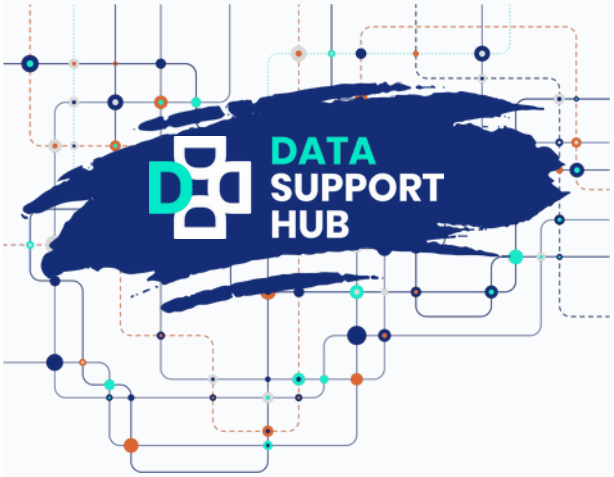
The Pitfall

Neglecting to train employees on UK GDPR requirements, handling data securely and data protection best practices can result in unintentional breaches and non-compliance. With 88 % of reported UK data breaches caused by human error, and the cause of 37 %1 being sending sensitive data to the wrong recipient, failure to train staff can have significant. consequences.

The Solution

Ensure staff are trained on GDPR principles, data protection policies, and their specific responsibilities. This training should be repeated regularly, at least annually. Online learning is effective in keeping employees up to date, informed and vigilant whilst remaining competitively priced. Provide staff with the organisation's data protection policies and procedures so that they can be referred to at any time. A well-informed workforce is a critical component of a robust GDPR compliance strategy.

1: www.verdict.co.uk/uk-data-breaches-human-error



Conclusion

Achieving GDPR compliance is an ongoing process that requires vigilance, education, and a proactive approach to data protection.

By avoiding these common mistakes and implementing the recommended solutions, businesses can effectively navigate the complexities of UK GDPR and mitigate the risk of non-compliance.

Data Support Hub's platform offers a comprehensive solution, including training and compliance tools, to ensure your business remains compliant and secure.

Remember, the cost of compliance is significantly lower than the potential fines and reputational damage resulting from a data breach.

Stay informed, stay compliant, and safeguard your business and its reputation with Data Support Hub.

SAFEGUARD your business TODAY

LEARN MORE

CONTACT US

VIEW DEMO