Founder Focus: FAQs for Start-Up Success

Start-Ups and Data Breaches

In today's digital age, data is a valuable asset for businesses, including start-ups. Start-ups, especially those handling personal data, face unique challenges when it comes to safeguarding sensitive information. Whether you are building a tech product, offering a service, or handling client data, understanding what to do in the event of a data breach is critical.

Understanding Your Obligations with Personal Data

The UK GDPR's broad scope means it applies to any UK organisation, regardless of size, that processes personal data. Compliance with the UK GDPR is non-negotiable. Non-compliance could lead to significant reputational damage as well as costs in the form of management time and potentially financial penalties. Demonstrating compliance and a clear understanding of the risks from the outset increases customer and stakeholder trust.

Start-ups often collect and process personal data from the outset – data of investors, clients and employees. Personal data includes names, email/ postal addresses, ID documents, financial details and even IP addresses. There could also be 'special category data' relating, for example, to people's health, racial or ethnic origin or genetic or biometric data, which is more sensitive and demands additional protection under the law.

Key legal obligations relevant to minimising the risk of breaches include:

— Only collect and store data genuinely needed for your business.

— Invest in and implement safeguards to protect data, relative to its sensitivity and volume.

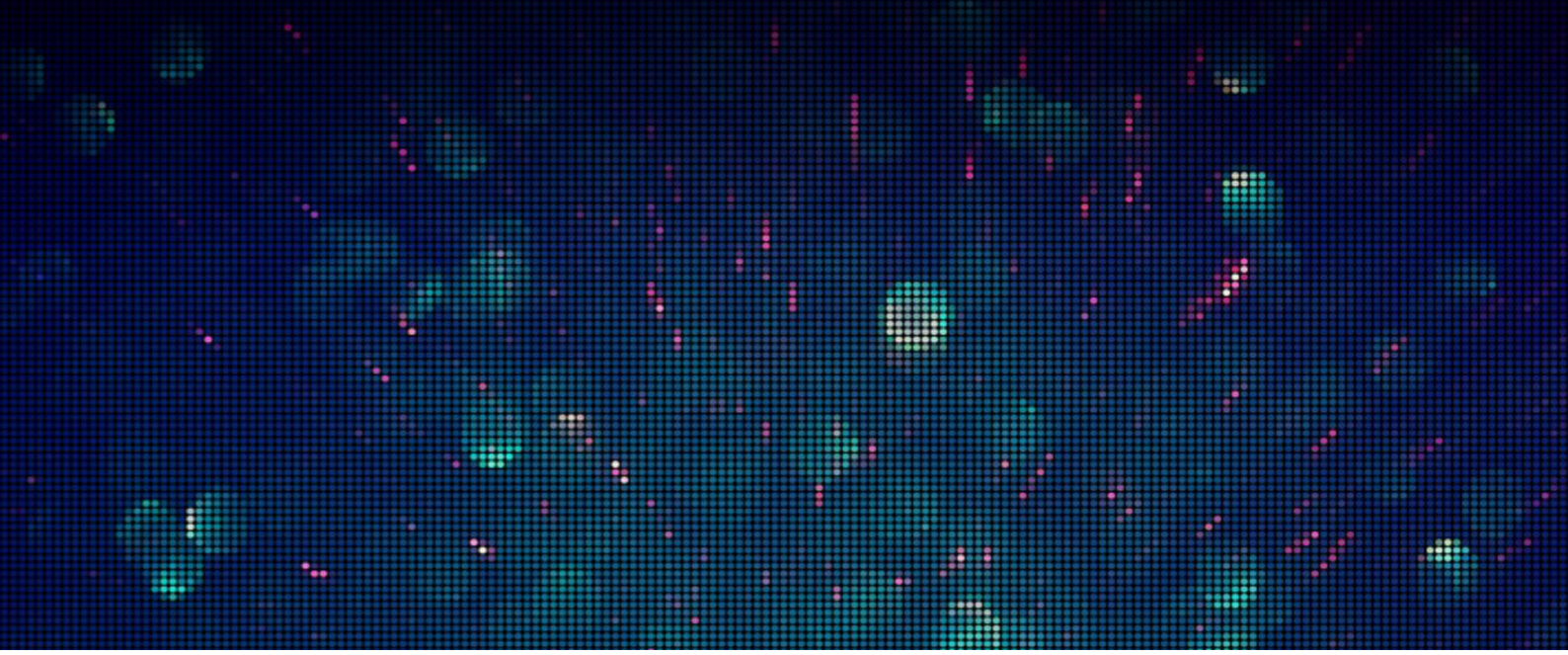
What Constitutes a Data Breach?

A data breach is not limited to unauthorised access to a system. It is defined as a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Therefore, as well as malicious attacks on an IT system, breaches can arise from doing things such as sending personal data to the wrong recipient or giving access to an unauthorised individual, or misplacing a device containing personal data. Start-ups must be able to identify and promptly address any forms of data breach.

Implementing Appropriate Technical and Organisational Measures

Start-ups must invest enough time, money and energy into ensuring that appropriate security measures are in place to guard against data breaches. This could include using encryption, access controls, and doing regular security audits. The measures that are put in place initially should then be monitored and assessed periodically to ensure that they evolve with the company.

As is the case for all businesses, a start-up should develop a procedure enabling them to promptly detect, report, and respond to data breaches. Where there are very few employees, short on time and resources, implementing suitable processes from the outset can make things easier in the long term.



While start-ups face unique challenges, such as rapid scaling and limited resources, they also often have the advantage of being able to adopt the latest technologies and best practices from the outset. To protect personal data, start-ups should:

— **Risk assess:** Identify potential vulnerabilities and assess the potential impact of data breaches.

— **Implement access controls:** Develop controls around who can access personal data.

— **Use encryption:** Encryption can be used to protect data both in transit and at rest, particularly more sensitive data.

— **Plan:** Prepare a data breach response plan detailing the steps to take if a breach occurs. Maintaining a hard copy of that plan is worthwhile in case IT systems are compromised and an electronic copy cannot be accessed.

— **Train employees:** Educate staff on data protection compliance and the importance of safeguarding personal data. Many breaches arise due to human error.

We have a Data Breach – What Now?

Not all breaches need to be reported to regulatory authorities. In the UK, certain breaches must be reported to the regulator (the Information Commissioner's Office) within 72 hours of becoming aware of them. Determining this requires assessment on a case-by-case basis. Affected individuals must be informed without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

The consequences of a data breach can be severe, including financial penalties, legal action, and reputational damage.

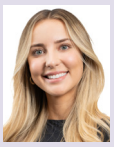
Any data breach suffered is an opportunity to learn and improve. Start-ups should log all breaches, recording the nature of the breach, its impact, and the steps taken to address it – enabling them to identify patterns and prevent future breaches.

Conclusion

Navigating the complexities of data protection compliance is a daunting yet essential task for start-ups in the UK. From understanding the legal framework and evaluating data handling practices to implementing security measures and responding to breaches, compliance requires a thorough and proactive approach. If a start-up is uncertain about its compliance status, it should seek legal advice from CMS to ensure that it complies with the legal requirements.

Any questions? Get in touch with the legal team

Jennifer Barr
Senior Associate
T +44 141 304 6233
E jennifer.barr@cms-cmno.com



Helena Siebenrock
Trainee Solicitor
T +44 131 200 7503
E helena.siebenrock@cms-cmno.com