Acacia Solicitors

ARTICLES

Acacia

Solicitors

Contact Person

DOLAPO ALAO ESQ
MANAGING PARTNER
dolapo.alao@acaciasolicitors.com

Taiwo Kehinde
Mosunmola ESQ
ASSOCIATE
taiwo.kehinde@acaciasolicitors.com

Data Is an Asset, But It Comes With Responsibility: Data Protection for Startups

Data as a Business Asset

Data has become one of the most valuable resources in the digital economy. For startups, it can inform product development, improve customer experience, support decision making and create entirely new business models. In many technology driven businesses, data is not simply something collected in the course of operations. It is part of the value proposition itself.

But there is an important side to this conversation that startups cannot afford to overlook. The value of data does not remove the responsibility that comes with collecting and using it.

The Responsibility That Comes With Data

As Boyacioglu and Yıldız observe, information has become a vital asset for emerging businesses, particularly as technology and business models increasingly depend on the collection and analysis of information. At the same time, the use of personal data creates a tension between commercial interests and the privacy rights of individuals.

This tension is particularly important for startups because they often operate with limited resources while trying to grow quickly. Data protection can therefore be viewed as something to deal with later, when the business has more customers, more employees or more funding. That approach, however, can create significant problems.

A startup may collect names, telephone numbers, email addresses, location information, financial information or other personal data without fully considering what happens to that information after collection. The important questions are not only how the data is collected, but why it is collected, how it is used, where it is stored, who has access to it and when it should be deleted.

Data Protection Is Also About Trust

Data protection is not simply a compliance exercise. It is also a question of trust.

Consider a simple example. A startup collects information from customers for a particular service. If that information is later used for an entirely different purpose without an appropriate legal basis or proper transparency, the problem is no longer merely technical. It becomes a question of whether the business has respected the expectations and rights of the people who provided that information.

This is why startups need to understand the concept of the data lifecycle. Data should not simply enter a business and remain there indefinitely. Businesses need to understand what information they hold, why they hold it, how long they need it and how it should be securely disposed of when it is no longer necessary. Boyacioglu and Yıldız emphasise the importance of businesses being able to account for where personal data is stored and to maintain control over its lifecycle.[i.]

The Cost of Getting It Wrong

There is also a broader business consideration. A data breach or poor data handling can affect more than regulatory compliance. It can damage customer confidence and the reputation of a business at a stage when trust may be one of its most valuable assets.

Research on startups has similarly identified the potential for data protection failures to result in financial and reputational consequences, particularly for smaller businesses for whom individual customers can be critical to survival.

For a startup that is still trying to establish credibility, losing customer trust can have consequences that extend far beyond any immediate regulatory response.

Data Protection Should Start Early

This is where legal advice becomes particularly valuable.

Data protection should not begin when there is already a breach. It should be considered when the product is being designed, when contracts with vendors are being negotiated, when customer information is first collected and when the business begins considering new uses for its data.

A data lawyer or privacy focused legal adviser can help a startup think through these questions, develop appropriate policies, structure data related agreements, identify risks and prepare for potential incidents.

Building With Trust

For founders, the lesson is simple.

Your data may be an asset, but the people behind that data are not merely data points.

Building a successful digital business therefore requires more than learning how to collect and use information. It requires understanding the responsibility that comes with having access to it.

The startups that take data protection seriously from the beginning are not simply trying to avoid penalties. They are building businesses around trust, accountability and sustainable growth.

And in a digital economy where trust can determine whether customers stay or leave, that is not just a legal consideration. It is a business strategy.

Practical Data Protection Process for Startups

1. Identify the data you collect

Start by identifying the types of personal data your startup collects, such as names, email addresses, phone numbers, financial information or location data. Also determine where the data is stored and who has access to it.

2. Define the purpose

Be clear about why each category of data is being collected and what it will be used for. Data should not be collected simply because it might be useful in the future.

3. Establish a lawful basis

Determine the appropriate legal basis for processing the data under applicable data protection laws. Depending on the circumstances, this may include consent, contractual necessity, legal obligation or legitimate interests.

4. Inform the data subjects

Users should be given clear information about what data is being collected, why it is being collected, how it will be used and, where relevant, who it may be shared with. This is where a clear and accessible privacy notice becomes important.

5. Control access and protect the data

Access to personal data should be limited to people who genuinely need it for their work. Startups should also put appropriate technical and organisational measures in place to prevent unauthorised access, loss or misuse.

6. Set retention periods

Determine how long different categories of personal data need to be retained based on the purpose for which they were collected and applicable legal requirements. Once the data is no longer necessary, it should be securely deleted or otherwise disposed of.

7. Prepare for incidents

Startups should have a basic process for identifying, containing and responding to data breaches or other security incidents. Knowing what to do before an incident occurs can significantly reduce its potential impact.

8. Review regularly

Data protection should evolve as the startup grows, introduces new products or changes how it processes[2] information. Regular reviews help ensure that the company's practices remain appropriate and compliant.

Endnotes

1. Cumhur Boyacioglu and Orkun Yıldız, ‘The Impact of Data Protection Regulations on Start-Up Enterprises’ in Orkun Yıldız and others (eds), Recent Developments in Individual and Organizational Adoption of ICTs (IGI Global 2021) 120, 120–133.

2. Eko Innovation Centre, ‘Why Ignoring Data Protection Compliance for Tech Startups Could Cost You Everything?’ (13 July 2026) https://ekoicentre.com/articles/why-ignoring-data-protection-compliance-for-tech-startups-could-cost-you-everything/ accessed 17 August 2026.
i.

3. Promise Legal Staff, ‘The Role of a Data Lawyer for Startups and Businesses: Protecting Your Digital Future’ (26 July 2025) https://blog.promise.legal/startup-central/the-role-of-a-data-lawyer-for-startups-and-businesses-protecting-your-digital-future/ accessed 17 August 2026.

1
2