



Access
Partnership

DELTA
Energy & Environment

Walking in the Footsteps of Tech Giants:

Eight Lessons Energy Companies Can Learn From the Tech Sector's Mistakes





Introduction

The energy sector is a relative latecomer to digitalisation, giving it the chance to learn from mistakes of others. However, as the sector moves to modernise its infrastructure and take advantage of the huge quantity of customer data it has access to, it risks moving from a legacy of politicised regulation and high stakes interventions around oil and energy into a tech sector where the same characteristics are increasingly appearing around data.

Considering the history of the energy sector and the lessons learned by tech companies, what are the eight questions these companies should be asking themselves?

Do you have a product or service that you are sure consumers will want?

We've found that energy is a need. What customers want is comfort, peace of mind and lower bills. Historically energy suppliers have been effective at supplying the energy but less successful at providing customer friendly services. We can change this now as suppliers embrace digital communication channels, new technologies like smart meters, and data-based offerings that help customers find the service they want.

However, one of the most critical mistakes made by the technology sector has been arrogance. Passionate about the benefits of technology, engineers adopted a blinkered vision with an illusion of absolute consumer demand. As a result, the sector dismissed cultural, regulatory, and political objections as Luddism. New technology providers have failed to consider these concerns in advance of a product launch or to address them as soon as they arise. The lesson learned — don't assume your product is so fabulous and consumers will desire it so much that regulators won't shut you down. They will.

Have you ever talked to your regulator or government about your technology product or service?

The technology sector has opted repeatedly to introduce products based on functionality without a broader legal-political product analysis, leaving the industry in a defensive position. Today, more sophisticated technology manufacturers integrate legal and political factors early in product testing stages to ensure workarounds for legal and regulatory concerns are addressed in advance of a product launch. A smart provider of technology solutions will take the step of previewing their product or data collection efforts with relevant regulators. If you are collecting data or deploying new technology, even as an energy company, you should consider these factors.

Politics has been, and will remain, a major driver shaping the energy industry. A core competency of energy suppliers is their capability to operate within a highly regulated industry context, and to influence the future direction of national regulation and policy. Therefore, close contact between energy companies and their local regulator is essential, particularly with most regulators intending to modernise the energy sector. Providers that don't ask this question risk being tossed onto the rocks by eager but poorly informed policy-makers, particularly as digitalisation introduces new competencies and responsibilities for energy companies.



Do you provide an international service?

A key failure in the technology sector has been in its inability to think beyond borders. Initial product development is often with a specific market in mind, but with the internet, technology and data are intangible, borderless assets. More than one tech company has been surprised to learn their products are being used by multinational customers in a market in which they do not operate or provide service, or in which they may not be licensed to provide service. To best protect your company against movement of technology or data out of its planned legal jurisdiction, think globally from the start. Plan your business and regulatory strategy anticipating your technology or data will leave the country.

In many ways, there is no such thing as a global energy supplier: the nature of the energy retail business is inherently local. Customers live in different types of home, in different climatic conditions and have different cultural factors that influence the way they use energy. Nevertheless, energy retailers can turn this into a key advantage. Each market reacts to unique conditions, creating testing grounds for new approaches and innovation that can be exported from local markets to international ones through B2B2C models if providers think cross-border.

What is your cybersecurity strategy?

A reality of any increase in technology use is an increase in technology vulnerability. Technology companies are at the forefront of handling cybersecurity challenges, but in some cases, it has taken a series of high-profile breaches to move the cybersecurity ball forward. The ensuing loss of customer confidence can be extremely damaging for a business.


Further, for the energy sector, an additional challenge may exist if a regulator declares the sector “critical infrastructure”, carrying more challenging cybersecurity requirements and corresponding penalties for noncompliance. The more you adopt technology, the more cautious you must be to protect your network and data and to comply with existing regulation.

The energy system is becoming increasingly interconnected through digitalisation and the rapidly evolving ‘energy Internet of Things’ which is creating new and more complex cybersecurity challenges for energy companies. With critical infrastructure at stake, the risks go beyond corporate data storage to affecting public safety, environmental stability, or economic prosperity.

The EU’s Global Data Protection Regulation (GDPR) legislation introduced in 2018 is well known, but as significant is the introduction of the Network and Information Security Directive (NISD), which applies to energy companies — including generators and network operators — and requires member states to introduce policy and regulation to achieve a high level of security of network and information systems. Energy companies need to be aware of NISD requirements throughout their supply chains and of member state-specific obligations. The industry must develop strategies to meet compliance requirements and to protect its assets and its customers from increasing cyber threats.

Do your customers know you are collecting their data?

One of the early failures of the technology sector — and for some companies, current failures — is not informing their customers how they are collecting and using their data. Notification requirements exist in most modern privacy laws today, focusing on the data, not the technology. So, if you are collecting customer data, you may be liable. Even if you are not liable, be aware that one of the greatest barriers between the tech sector and its customers today is trust. As any good business knows, losing consumer trust means losing business.



Even with full compliance, risks remain. Let's assume your organisation is fully GDPR compliant, with first-rate communication and transparency around customer data. Now ask yourself what proportion of your customers actually read the terms and conditions they've signed up to. How about the relevant section which lays out how you use customer data? Even if they have read it, do they know precisely what data is collected? And are they aware of and fully understand the implications of this? The deeper you go, the less customers know, and they may be shocked to discover how their personal data can be used. Energy companies wanting to innovate and deepen relationships with their customers may find themselves the recipient of consumer backlash and must have a contingency plan in place.

How do your data, legal, and product teams interact?


At its early stages, the legacy mentality of “engineers rule” within tech companies meant that engineers had business leadership roles but failed to consider commercial, legal, and consumer issues attached to their products. With increased regulation, tech companies have required a level of internal coordination to guarantee that the products and data collection processes are compliant with national and regional laws and address prevailing political concerns. Energy companies should ensure an internal coordinative structure across its value chain to avoid legal or commercial backlash.

Conversely, data, product and legal teams can often be quite remote from each other in the energy sector with different reporting lines and representation at Director level. This in itself is fine, but should flag the need to form, strengthen or maintain good lines of communication between appropriate departments. For example, cross-functional virtual product teams can help raise and discuss issues and meet the GDPR's privacy-by-design guidance. Formal governance procedures at relevant product ‘stage gates’ can also serve to ensure compliance and protect customers and company alike. Putting this in place from the start can also give competitive advantage through quality of solution and speed to market.

Are you aware of all that your company is doing with customer data?

Some of the more recent technology industry problems around handling of customer data are due to decision-makers' lack of awareness of what engineers or technical teams are doing to manage data. A decision made by an engineer to reroute traffic or to collect data for the sake of efficiency or for improved product outcome is a normal business process. But, without awareness of those actions and their ramifications, corporate leadership cannot keep the company safe from cyber risk and increasing penalties. If you are the chief legal officer or the CEO, the decisions of technical or product teams may have a major impact on your business. Therefore, it is critical to assess risk and approve product, compliance, and regulatory strategies.

How rigorous was your company's data inventory as an early step towards gaining GDPR compliance? Did it cover all data storage locations, including legacy systems, department files, spreadsheets, memory sticks with employees' own extracts and analysis, and third-party cloud provision? How robust is the access criteria, encryption and sharing of such data? Then do you know who uses it for what purposes? Does data processing, whether internally or by partner organisations, incorporate personalised customer data of those who have opted-out? Decision-makers in the energy industry should have the answers to these questions as they might be confronted with them by regulators or the general public.



How much external support do you use for product development? For compliance?

The technology sector initially failed to solicit help. As the industry was largely unregulated in its infancy, there was no culture of compliance to build on or that understood the need for external support. However, that is not the case today. More and more technology companies seek outside assistance and are doing it earlier in the product life cycle and despite the size of the company, with clear results.

Similarly, energy companies have historically been quite insular, keeping most work in-house. But collaborating externally has many benefits for areas like product development and compliance. You can enlist support from leaders in your field, gain fresh perspectives and learn from and adapt best practice in other sectors. External specialists not only have experience to benefit from, but they are also likely to have their finger on the pulse and help you be proactive in responding to changing needs and circumstances. Energy companies should not be afraid to reach out and collaborate externally; indeed they should embrace it.

Conclusion

Navigating technology and data rules is highly complex. The most prudent technology users must work with telecom licences, IT ministries, data providers, and vertical regulators — in this case an energy regulator. Companies at all sizes find that they cannot alone understand the myriad of technology regulations impacting their businesses in over 200 countries. As technology use and data analytics increases within the energy sector, these obligations become your obligations. Reach out to the experts.



Access Partnership is the world's leading public policy firm for the tech sector.

Laura Sallstrom
Global Head of Public Policy
laura.sallstrom@accesspartnership.com
+1 202 503 1570



Research and consulting services helping organisations to develop the best strategies, business models and customer propositions for the energy transition.

Andy Bradley
Director
andy.bradley@delta-ee.com
+44 (0)131 476 4259