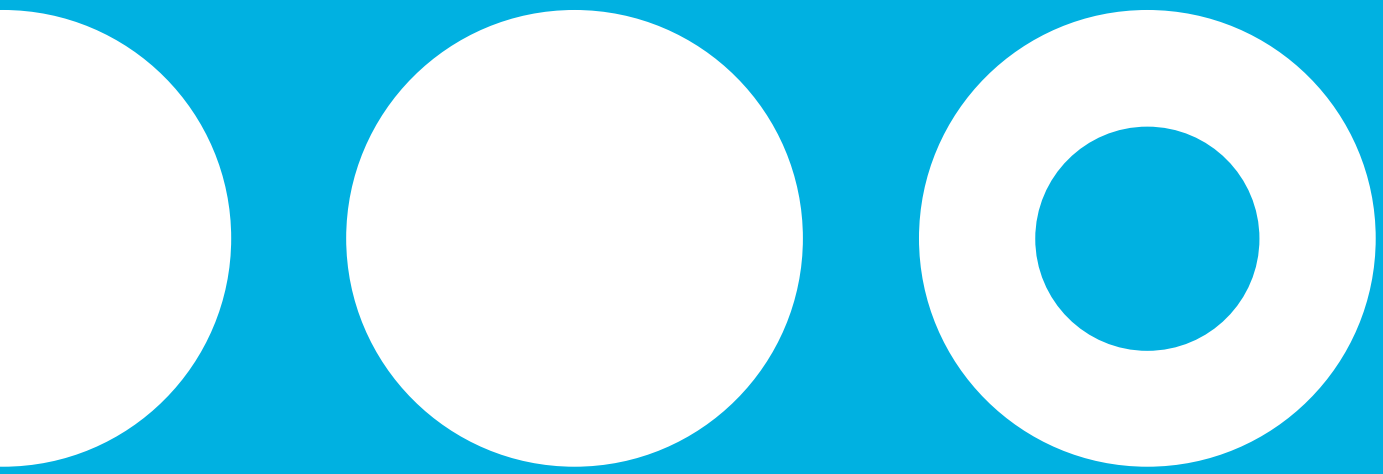
White Paper:

Data Protection Concerns for Start-ups & Challengers in the U.K. Energy Sector

October 2018



chaucer...

AUTHORS:
Robert de Souza and Paul Gillingwater, from Chaucer's Data Protection team

www.chaucer.com/digital

Contents

Introduction

IN THIS PAPER, WE WILL CONSIDER WHAT SPECIAL CONCERNS ARE FACED HERE IN THE U.K. BY START-UPS AND CHALLENGERS, ESPECIALLY (BUT NOT EXCLUSIVELY) THOSE IN THE ENERGY SECTOR.

Organisations are becoming highly dependent on smart data analytics drawn from smart home products such as Hive, Amazon Alexa and Philips Hue to provide tailored products and services to their customers.

Emerging technologies for the home and the introduction of the Internet of Things continues to open up new opportunities and new markets for utilities, Big Data and connected devices such as smart meters are set to transform the utilities sector, making it highly responsive, competitive and offering better value for customers.

New Regulations in the UK

The EU's new General Data Protection Regulation (GDPR 2016) and the UK's Data Protection Act (2018) demand a high level of sophistication in data management and protection that will not just dominate the utilities sector but all sectors where personal data is collected and/or processed. Together with the EU's NIS Directive, which imposes stronger cyber security measures and reporting obligations, these laws impose a significant new compliance burden.

These three pieces of legislation now set a very high standard throughout the EU and within the UK for the protection of personal data. Together, they deliver a universal legislative framework of instructions for businesses, covering key areas such as consent, data portability, the right for customers to be "forgotten" and Subject Access Requests (SARs), which by definition put the control of personal data back into the hands of the data subject. With this list also comes the threat of fines of up to four per cent of global annual turnover, or up to €20 million for serious non-compliance.

Meeting the mandatory high standards set out within the legislation will mean significant investment for the utilities sector, where many of these businesses run core infrastructure and systems that have not been designed to meet the needs now expected when being the gate-keeper of personal data.

Mission Critical Privacy

Transformation of these systems has moved from 'nice to have' to 'mission critical'. Furthermore, through the introduction of 'Privacy by Design' there is a mandatory expectation that proper respect is given where personal data is present within the transformation programme. It's essential that the business systems development program takes on board the lessons of good privacy design, and ensures that project managers refuse to bring new systems online unless privacy is assured—and that means requiring DPIAs to be prepared for all new systems that process customer data.

The legislation will ensure that businesses are, and remain, fully accountable for the personal data they hold. It will further ensure that the right investment is made in technology, to support the processes, procedures and policies, newly established and executed, to protect personal data. This will, in turn, allow businesses to harness that data in ways that can transform customer communication, develop new markets and increase revenue.

Ultimately, this will make the utilities sector more transparent, trustworthy and able to have more meaningful targeted conversations with its up-to-date, clean and managed customer database.

Smart Meters

The roll-out of smart metering and in-home sensors such as Hive aim to help businesses better serve and inform their customers. But this hinges on being able to process the data that these connected devices collect – something that, up until now, the utilities sector has not been able to perfect.

Investment in GDPR compliance should be targeted to produce systems, as well as the understanding and expertise, needed to do this.

Businesses will need to get these data records in order, understand what has been stored, and how different departments are using customer data. They will also a need to maintain a strong audit trail of permissions that customers have given for use of their data, and how this information flows through an organisation, to be able to fulfil the key principles set out in the regulation.

Data Portability

Take, for instance, the 'data portability'[1] requirement that stipulates that data can be transferred to a new 'controller' at the request of the 'subject'. When switching energy supplier, a customer can request that all data held on them by their original provider be transferred to the new one and that any record of that data then must be forgotten.

To meet these requirements, companies will need to become more versatile and able to share and compartmentalise data more efficiently. This will open opportunities to use data to improve customer communication. For instance, combining usage data from smart meters with a customer's postcode might enable the company to provide them with geographically relevant information on the most cost-effective times to turn their heating on.

Equally, in-home sensors could provide early warnings of when equipment develops a fault or is operating inefficiently. Some IoT devices are now offered that can detect carbon-monoxide or smoke, thus offering critical safety services. Having robust IT infrastructure and data systems to back this up will be needed to give firms the back-office muscle they require to proactively communicate this information with customers in meaningful, simple and relevant ways.

Legacy IT

For some utilities companies, the investment to replace legacy IT systems will be unavoidably huge. This, along with Brexit uncertainty, goes some way to explaining why a lot of businesses have put off addressing the issue up until now.

This 'wait and see' approach is likely to be costly in the long term. We have seen in other sectors that companies that have "bravely" invested in the right customer systems are reaping the benefits of better engagement in higher customer satisfaction scores and greater speed to market. The GDPR is still likely to be the biggest influence on data protection in the UK after it leaves the EU, even for businesses who ply their trade solely within UK borders. As if to prove this point, the Queen's speech recently put forward plans for a Data Protection Bill that looks set to mirror the requirements of GDPR.

The truth is that GDPR sets out a benchmark for the use of customer data that all businesses should be working towards. For those that approach the challenge intelligently and proactively, the by-product of compliance will be a programme of work to recruit the right people and create the processes and systems they need to take full advantage of data to deliver great customer communication.

[1] The Article 29 Working Party issued Data Portability guidelines in 2016, saying: "The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another." This was seen as an important element of the European Commission agenda for the digital single market.

Employee Screening

Businesses such as energy companies which may from time to time send service agents into the homes of members of the public, need to ensure that they observe safeguarding laws, which means that such employees should have background checks performed. Depending on how such a check is performed, it can be highly intrusive in terms of personal data, and the company needs to ensure that such data is properly managed.

There are two choices: either conduct the DBS checks directly, or outsource the process to a specialist company. In both cases, your company would be functioning as a Data Controller for potentially sensitive special category data (i.e. criminal record status information), while in the latter case, the outsourcing partner would be a Data Processor.

One interesting factor – neither consent nor legitimate interests would necessarily constitute the lawful basis for processing possible criminal record data under GDPR. Rather, the Health and Safety Act (1974) might be used as a regulatory obligation to protect both staff and customers. Screening employees protects not only customer safeguarding, but also ensures that fellow staff members are protected from working closely with persons who might have criminal backgrounds.

Impact of Brexit

In March 2019, the act of Brexit will place the U.K. outside of the E.U.'s regulatory purview, and specifically for data protection purposes, the U.K. will be considered as a 3rd country. The presumption is that the U.K. will very rapidly be granted adequacy status, as several other countries have already received, such as New Zealand, Norway and Switzerland. Such a status confers the ability to cite the adequacy ruling as a so-called "transfer mechanism", where data is being transferred from within the E.U. back to the U.K.

In case such an adequacy status is delayed, (given that Japan's adequacy status has taken nearly two years to progress), prudent businesses will seek other transfer mechanisms, such as Binding Corporate Clauses (for transfers within a large multi-national), or more likely the use of Model Contractual Clauses, as approved by the E.U. Such clauses should be built-in to the Data Processing Addendum documents that are necessary between Data Controllers and Data Processors.

Transfer mechanisms may not be the only aspect affected by Brexit, as at the stroke of midnight, British businesses will be assigned 3rd country status, and may require EU representation when dealing with customers in the EU (such as the Republic of Ireland.) Cross-border delivery of energy is more effective when you're allowed to legally process the data of your customers on the other side of the border, so ensuring this functions well after Brexit is essential.

Customer Switching & Data Portability

A strict reading of GDPR suggests that every piece of personal data, including a five-year history of gas and electric consumption, is personal data, and therefore in scope for the right to data portability. Legacy systems are especially problematic in this regard.

The EU itself wants to encourage a competitive digital market, and therefore the portability of data was emphasized from the outset. This naturally conflicts with the desire of established utilities to retain customers, potentially by making portability more difficult. We predict that customers will give more trust to suppliers who are serious about supporting rights such as data portability.

Growth Hacking Safely

For the past few years, growth hacking has been seen as an important technique to turn startups into unicorns. Such hacks come in many forms, but are tend to be very focused on acquiring new customers, and their data. A recent court case shows that some hacks have the potential of leading to litigation. Ebay is currently suing Amazon for allegedly creating thousands of fake accounts on the former's platform, in order to "steal" their customers. While this may not be a breach of data protection, it does show that growth hacking is a serious business. Any company wishing to engage in such an activity should be very careful to observe data protection law, and ensure their proposed activity doesn't lead to a breach or infringement on data subject rights and freedoms.

Cloud Migration

If you have a legacy IT framework, top of the agenda will likely be a cloud migration. This brings its own set of risks, starting with unauthorized access, misconfiguration, and of course compliance. Most cloud providers have GDPR programs, but they mostly address the technical security controls rather than improving privacy management. In any migration scenario, a DPIA is essential before going ahead with such migrations.

ISO27001 and Setting Standards

Cyber security is absolutely essential for modern businesses, especially those categorized as being Operators of Essential Services (OES). The ISO 27001 standard for creating an Information Security Management System (ISMS) is not enforced by any law, but is strongly recommended as best practices in data protection thinking.

Budgeting for Cyber Security and Data Protection

Cyber security and data protection each require a significant investment, in people, resources and systems to get it to the level where risk is being appropriately managed. The big challenge for CISOs and CPOs is: how do you know when you've allocated enough budget? Where should you be spending to make the biggest impact?

Above all, do you have the right people in place, with the correct roles, and have you equipped them with adequate resources and training to mitigate both the known and unknown risks? It is these questions which more than anything will keep the C-Suite awake at night. Given the potential for massive reputational and regulatory risks associated with a significant breach, how much should you be spending? And is it possible to insure or transfer some of this risk?

For Operators of Essential Services, there is a 24-hour reporting obligation in respect to data breaches and other cyber security incidents that could potentially interrupt services.

2 https://www.pymnts.com/sizzlefizzle/2018/ebay-amazon-ecommerce-lawsuit-retail-funding-hackers/

Marketing Segmentation and Profiling

An important characteristic of modern data-driven start-ups and challengers is an increasing reliance on "big data", especially in regard to the profiling and segmentation of customers and prospects. GDPR takes very specific aim at ensuring that any profiling taking place is handled in a way that respects the rights of individuals, and businesses engaging in such profiling.

Ensuring that your marketing team is well-versed in legitimate processing and profiling in accordance with GDPR will help to minimize the risks of non-compliant activities. All new marketing initiatives should be run past your DPO before making what could be an expensive mistake—not just financially, but more importantly in terms of customer trust.

Dealing with Data Quality

One of the consequences of rapid growth is the possibility that data, especially that of customers, has not always been filtered and quality checked. For example, ensuring valid post codes are used, and that the post codes match street names.

Banking and Transaction Security

Data protection is not just for personal data, but also should consider the protection of your company's treasury function. This means implementing not only the traditional accounting controls of requiring multiple people to complete major financial transfers or payments, but also ensuring that the people with that responsibility are properly trained and have special protections against spear phishing that targets their function.

An example of an effective control is to enforce two-factor authentication on the system which can perform payment functions. Another example is to enforce review of any changes to bank details, e.g. any supplier who communicates, such as via email, to inform about a change to the bank account used to pay an invoice, should be very carefully reviewed and double-checked.

Data Governance

Most of the topics addressed in this white paper fall naturally within a data governance program. After getting top-level support from the board, and appointing qualified and experienced senior executives, we believe that more agile businesses will quickly discover that sound governance of the data holdings will have a multiplying effect on the company's business initiatives.

Outsourcing, Off-shoring and International Transfers

A special area for concern of GDPR is ensuring that data processed outside the European Union, which means in countries that might not have the same standards as those imposed by GDPR, could lead to increased risk. One of the obligations of GDPR is ensuring that such transfers are properly managed, and have the right lawful basis before signing contracts with offshore providers, especially those who may be processing customer information. This includes web analytics businesses, many of whom store their data in the cloud without a clear understanding of data residency rules.

Merger and Acquisitions

Challengers look for rapid growth, which if successful leads to them becoming an attractive takeover or acquisition target. Whether being an acquisition target, or considering acquiring another business, your company needs mature processes around and insight into your data protection practices. Specifically, if you're going to be acquired, it's important that you are ready at any time to demonstrate the effectiveness of your data protection controls and processes.

If you're planning to buy another company, then it's vital to carry out effective due diligence, and assess the potential risks of taking over a huge set of personal data which might not have been collected in a lawful manner.

Ensuring Accountability

Talk with senior managers about risk. Under the U.K. Data Protection Act (2018), senior executives, company secretaries and other key decision-makers are potentially personally and criminally liable for violations of data protection. This personal liability should change the relationship of board members and senior managers with respect to the importance of proper compliance, which should no longer be seen as merely a box-ticking exercise.

Valuation of Data

Have you considered the valuation of your data, and especially the personal data you hold which actually belongs to your customers and employees? Many M&A agreements ignore a proper formal evaluation of data, and if the appropriate legal language is missing from a sale agreement, this might be challenged by a court. Furthermore, it's important to consider, where consent has been granted to company A – when company B buys company A, is the consent they collected from customers fully transferrable, or do you need to re-paper your consent?

Consent may not be transferrable, but contracts certainly are, so perhaps Contract is a better basis for processing the personal data of customers. A recent legal case in the US is relevant here: the ratings company Nielsen is currently being sued by one of its major shareholders for allegedly making misleading statements about its GDPR readiness, that might affect the company's access to third party data, and therefore could potentially lead to a reduction in the company's value. This shows that GDPR is having legal effects even beyond its intended scope.

Conclusion

Data protection, and respect for the privacy rights of individuals, can no longer be ignored given the new regime of laws across the European Union. Brexit is unlikely to change this, given that the U.K. has passed its own Data Protection Act which will ensure continuity.

Challengers and start-ups in the U.K.'s burgeoning energy market have to establish greater agility in order to fuel their growth, but can only do so safely if they have a robust and effective program to comply with the new laws.