Data Protection as a Competitive Differentiator

Getting ready for the General Data Protection Regulation

SOGETI

“...For many online offerings which are presented or perceived as being ‘free’, personal information operates as a sort of indispensable currency used to pay for those services. Although there are a number of benefits associated with this, these growing markets pose specific risks to consumer welfare and to the rights to privacy and data protection.”[1]

Loyalty & Trust

Trust is the key to achieving customer loyalty and is itself attained through transparency, honesty and a respect for the individual. In the wake of international scandals such as Wikileaks and Ed Snowden’s outing of the NSA’s practices, one of the most effective ways to gain your customers’ trust is through ensuring the privacy of their data. Indeed 89% of consumers surveyed in the TRUSTe 2014 U.S. Consumer Confidence Index stated that they would avoid doing business with a company they felt was not protecting their online privacy.

In addition to this, the considerable legal financial penalties that can be incurred when a breach of privacy does take place, coupled with the potential revenue loss and customer churn, means that ensuring your customers’ data is well protected could be a key differentiator that puts you ahead of the competition.

89% of consumers would avoid doing business with a company they felt was not protecting their online privacy.

TRUSTe 2014 U.S. Consumer Confidence Index

Content vs Context

In the UK, the Data Protection Act 1998 (DPA) defines the legal requirements for the handling of personal data and outlines the consequences of not adhering to these conditions: *“...appropriate measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”*

This begs the question, what actually constitutes personal data? According to the ICO[2], the statutory definition is *“Non-automated records that are structured in a way which allows ready access to information about individuals.”*

Until recently the judgment in the case of Durant v Financial Services Authority[3] was the overriding precedent for more detailed guidance on what comes under the umbrella *“personal data”*. In this case it was deemed that *“personal data”* was information of *“biographical significance”* that had to go beyond a mere mention of an individual’s name in a matter which has no personal connotations, such as a meeting request e-mail. However, Durant has often been criticised for looking only at the **content** of the data and not at the **context**, therefore giving a narrow definition. More helpful is the Court of Appeal judgement in the recent case of Edem v The Information Commissioner[4] which states that to define personal data under the act we must look at the context of the data to see if a person can be identified.

For example if we just saw the name Jeremy Hunt on a database, as the name is fairly common the person is most probably not identifiable. However if other names on the list include George Osborne

[1] Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy March 2014

[2] http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

[3] http://www.5rb.com/case/durant-v-financial-services-authority/

[4] http://www.allenovery.com/publications/en-gb/Pages/Court-of-Appeal-endorses-Information-Commissioner-Office-Guidance-on-meaning-of-personal-data.aspx

To define personal data under the act we must look not only at the content, but also the context of the data to see if a person can be identified.

and Theresa May, or the database is named "Cabinet Ministers", then we know what we are looking at and we know that Jeremy Hunt is the Health Secretary. In other words, a name is always personal data if the context in which it appears is sufficient to identify the named individual.

How does this impact your business? Well it sets the bar higher for ensuring data protection and means that when you sit down with your lawyers to define your data privacy policy and strategy, you need to consider the context and juxtaposition of the data as well as the actual data content when determining whether or not you have fulfilled your obligations under the Act.

Introducing the General Data Protection Regulation

In 2012, the European Commission (EC) published its draft proposal for a General Data Protection Regulation (GDPR), a new pan-European Union standardised law to update and replace the Data Protection Directive of 1995, which was considered to be out of date in light of the growing number of US and European data breaches.

The Snowden debacle encouraged the EU to push the GDPR forward quickly and it looked set to become law in May 2014. However, the Regulation came under attack from external sources and, more surprisingly perhaps, from within the senior ranks of the EC itself. The UK lobbied to have the Regulation either downgraded to a Directive or abolished altogether, suggesting each nation should determine its own privacy laws based on national priorities and the possibility that the proposed restrictions will inhibit business innovation.

In light of this and a number of other obstacles, some people believe the GDPR may not come to fruition at all and others feel that, at the very least, it will be years before it is passed. So should your business simply continue with its current Data Protection strategy or should you begin to update your privacy policies now in early preparation for the Regulation?

Revising Your Privacy Policy

Whilst we are now aware that data protection and privacy are crucial to your customers' desire to do business with you, a 2008 report by McDonald and Cranor found that online privacy policies are typically so cumbersome and onerous that it would take the average person about 250 working hours to actually read all of the privacy policies of the websites they visit in a year.

Digitalisation and Big Data have only made data protection more complex and difficult to achieve in the last 6 years and there have been few major amendments to the DPA during this time, save refinements made by the Privacy and Electronic Communications (EC Directive) Regulations 2003, which altered the consent requirement for electronic marketing to *"positive consent"* (i.e. an opt in box rather than an opt out). This means that any existing privacy policies aren't truly in line with the current law, let alone prepared for the GPDR or designed to promote customer loyalty.

Businesses that are not already updating their privacy strategy and making their policies more customer-friendly are missing an opportunity to differentiate themselves in a way that customers currently deem to be very attractive.

If the potential to win more customers isn't a sufficient incentive to start preparing for the GDPR then perhaps the heavy sanctions will be. The penalty for a breach of the GDPR will be a highly significant €1 million or up to 2% of your global turnover. Speaking in 2014, ICO Deputy Commissioner, David Smith, expected the GDPR to be enacted at 2017 at the earliest but advised, *"Get your house in order now, under the current law, to ensure you are ready for the coming changes, because the principles are not very different."*

Another major advantage of revising your privacy policy now is that you can spread the work and the cost of compliance over the next 3 years before the GDPR comes into play. The bottom line is that the potential sanctions for non-compliance with the Regulation are so severe that it makes sense to ensure your privacy policy is up to scratch in the next 3 years, and the benefits of improving your privacy policy are so great, that regardless of whether the Regulation comes into force or not, it's a worthwhile undertaking.

Businesses that are not already updating their privacy strategy and making their policies more customer-friendly are missing an opportunity to differentiate themselves in a way that customers currently deem to be very attractive.

A key question to ask yourself at each stage is: *"Is it reasonable to assume that a member of the public would expect their data to be used in this way?"*

10 Ways to Prepare for the GDPR

1. Do a full audit, take a complete inventory of all your data and create a map of data usage.
2. Ensure that your new strategy is designed around the concept of obtaining explicit consent for all personal data usage and lifecycle.
3. Create a solid data breach system with clear processes and procedures in the event of an unavoidable or accidental breach.
4. Ensure that data loss reporting is fast and thorough as this will become mandatory.
5. Get the whole Board involved and create a culture of privacy and protection so that it is embedded in every part of your business and every member of staff understands the importance of compliance.
6. Appoint a Data Protection Officer - either part time or full time depending on your business requirements, quantity of data, data usage and data testing.
7. Choose a framework that suits your business such as ISO, NIST, or COBIT.
8. Monitor your new system and utilise comprehensive reporting, ensuring it is adjusted accordingly so it works for your business and your customers.
9. Rewrite your privacy policy and make it accessible on your website so that it is user friendly and your customers can find it and easily understand it.
10. Ensure that you are using data obfuscation and data encryption & decryption at every stage in your test environments in order to maintain integrity, privacy and data protection.

Managing Privacy in a Test Environment

It is very possible that a failure to test a fix in a test environment could result in errors being introduced into the live environment, which could then result in a breach of the DPA. However, testing itself creates a variety of scenarios where a breach of data privacy is possible.

> *"Businesses should not rush products and services to market without thorough testing and they should listen to their privacy advisors before giving into pressures from the marketing department."*
>
> David Smith, Deputy Commissioner, ICO

It is therefore essential to ensure that you extract only the data required for testing and then employ a variety of data obfuscation techniques such as data substitution, number variance, gibberish generation, data masking and synthetic data, in conjunction with encryption. This keeps the data realistic and testable but hides information from internal staff like the development and testing teams.

If obfuscated data is lost, a non-authorised user would not be able to ascertain the details of any individual so a breach would be avoided. Your chosen data obfuscation strategy needs to be carefully evaluated to make sure that the data is still suitable for testing, to establish how impenetrable the scrambled data is if under attack, and to determine how much the strategy will cost. For example, if you're testing an application that requires data validation, data substitution may be a simpler, faster and more cost effective means of obfuscation than creating synthetic data.

End-to-End Test Data Management

The importance of testing increases in parallel with the ever rising expectations of your customers. In light of the complexities of data protection and the potential changes to the law, we've seen that it's essential that your test environments are secure.

Outsourcing to a business in which Quality Assurance is a core competency is a sensible way to ensure speedy, efficient and secure testing with the right level of encryption and obfuscation to give you total peace of mind. Sogeti offers a complete end-to-end level of data encryption and Test Data Management (TDM) Service that:

- Analyses organisations' current software testing and test data management.
- Proposes what actions and toolsets are needed to improve testing.
- Helps customers to choose the right testing tools.
- Offers a pilot or proof of concept to show that the selected tools can deliver the test data required and that the proposed process can deliver the expected benefits.
- Provides a full TDM rollout.
- Supports and trains customers all the way through the process and even after the rollout.
- Ensures that the number and size of the test environments are precisely what is required by introducing a smart solution to make sure that the right data is made available for testing.

With our forward-thinking, comprehensive TDM service, we can help you ensure you are delivering quality and value to your customers while conforming to the existing and impending legislation.

Case Study: Government Institution

Challenge

The client was looking to comply with privacy regulations banning the use of production data in test environments. Knowledge of data structure and business knowledge of applications was limited within the institution. Their goal was to set up a process and corresponding TDM service where test teams could acquire masked test data sets for use in testing.

Solution

Sogeti demonstrated in a proof of concept (POC), together with a tool supplier, how in a short amount of time masking and sub-setting could produce functionally correct data sets for use in test environments. The TDM approach has since been rolled out to the entire organisation including tooling, training and support.

The client has now achieved compliance with EU and country-specific privacy regulations. Other benefits include an improvement in the quality of their end-to-end test data, an 80% reduction in the size of test environments due to sub-setting, and a 66% reduction in set-up time for preparing test data.

Why Sogeti

Sogeti has extensive proven experience in helping our clients around the globe to deliver high quality applications. Our staff provide ongoing support and engagement throughout the project, helping to drive higher quality testing standards and practices.

Sogeti's close partnerships with leading technology firms means we are able to offer guidance and advantageous pricing on a wide range of both premium and open source tools, and platforms. We also offer a range of innovative consumption-based pricing models, allowing you to eliminate large upfront investment and guarantee predictable outcomes.

About Sogeti

Sogeti is a leading provider of local professional technology services, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cyber Security, combining world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 20,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Contact us

T. 020 7014 8900
E. enquiries.uk@sogeti.com
W. uk.sogeti.com

facebook.com/SogetiUK blog.uk.sogeti.com twitter.com/uk_sogeti