Data Breaches: the business risk of the decade

Working across the information space in both the private, not for profit and the public sector, The Trust Bridge Senior Consultant, Carol Tullo, has seen the ecosystem of data policy expand and collide with the world of information rights. Carol states that "So many of us operating in this field have balanced the advantages of the open flow of data with the tensions in the safety and compliance safeguards that we expect, be it as individuals, family units or businesses"

The access, storage and tracking of personal data has changed our worlds. Protecting our data and our individual profiles is what data protection is all about. This is not new.

Data protection legislation has been on our statute book since 1984 when it was described as *"[regulating] the use of automatically processed information relating to individuals and the provision of services in respect of such information".* That language seems very dated now, but of all the legislation accessed online with millions of users each year, the Data Protection (DP) provisions remain number 1 in the legislation Top Ten! That is an illustration of how pervasive DP is in modern understanding and why the implications of the changes will affect every citizen.

The legislation was updated across the EU in May 2018 with the introduction of the GDPR (General Data Protection Regulation).

GDPR is not new but it recognises that new controls are required as data is layered onto data and collections of information grow ever more complex.

The safety of online content and the encouragement of technology companies to protect users' data is part of making the digital world safer.

Elegant solutions that allow businesses to future proof their data holdings and prepare themselves for this new world are required.

This is all about building on what you have already done, getting organized– in other words being smart and prepared.

However, in the pressures of the day job and other business deadlines, housekeeping data systems is fairly low on the priorities of senior managers. The governance of what are key assets of the business is a business risk that should be on every organisation's risk register. In our experience, we find that when something goes wrong it focused senior minds on the importance of their information assets. There is now a regulatory need to escalate good practice and get that house in order. There is a lot of expert and experienced help to steer and guide business.

One area that should be upper most in the mind of all senior managers is that of data breaches – highlighted by the cases of Equifax the global information solutions company, in 2017, which eventually reported a major cybersecurity incident affecting 143 million consumers in the USA. The breach is thought to have revealed the names, Social Security numbers, birth dates and addresses of almost half the US population. UK and Canadian customers were also affected. More recently, the international hotel group Marriott announced on November 30 2018 that they had exposed the records of 500 million customers in a data breach, stating that their guest reservation system and database had been

hacked. The personal data of those 500 million guests, who have stayed in their hotels across the world since 2014, had been accessed. On hearing this, many in the hospitality sector reacted with horror.

In fact, a mere 2 weeks later, on December 14th, Facebook announced that a software bug allowed a 3rd party developer to access the photographs of nearly 7 million Facebook users, regardless of whether these photos had been shared or not.

One of Britain's largest retail franchises, CEX, disclosed earlier in 2017 that it had been hit by a data breach that could have compromised the information of as many as 2 million customers – including personal details like names and addresses.

Bupa has suffered a data breach (13 July 2017) affecting 500,000 customers on its international health insurance plan and Wonga's data breach could have hit as many as 245,000 of its customers including bank account numbers and sort codes.

Late in 2016, Tesco Bank froze its online operations after as many as 20,000 customers had money stolen from their accounts.

In this world where we all rely more and more on technology and the data economy, we as individuals need to be able to trust that those with whom we share our private information can be trusted to keep it safe. This is one of the main motivations behind the drafting and implementation of the General Data Protection Regulation or GDPR.

All organisations will be required to focus on data security and in fact should be doing so in order to avoid the costs and the reputational damage that data breaches may cause, and also to avoid the risk of hefty fines.

Under the GDPR legislation, all organisations will be obliged to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. As we have seen in recent high profile cases, this has not always happened in a timely fashion. Data breaches will attract very significant fines: up to €10,000,000 (US $ 11.5 MILLION) or up to 2% of the previous year's total worldwide annual turnover of the organisation, whichever is higher.

To examine this a little more closely, lets define what constitutes a data breach:

According to the Information Commissioners Office (the UK's independent authority set up to uphold information rights in the public interest) a personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data". A breach also refers to inappropriate access of data in the event that proper controls are not in place.

There is a requirement to report a data breach if it is perceived that there is a risk to the "rights and freedoms of individuals". This means that if a breach causes or is perceived to cause any financial loss, or by making the data public the individual's confidentiality is affected, or any type of discrimination could result, plus reputational damage. All such breaches would need to be reported to the authorities, and in some cases to the individual him or herself.

Security and breach reporting requirements are covered in Articles 32-34 of the GDPR (https://www.gov.uk/guidance/data-protection-bill-overview). Breaches are covered specifically in Article 33.

In Summary, this article states that personal data breaches must be reported to the Supervisory Authority "without undue delay and, where feasible, not later than 72 hours after becoming aware of it. There are exceptions to this time line if the personal data breach is deemed "unlikely to result in a risk to the rights and freedoms of data subjects"

The breach notification must detail the following information:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the relevant Data Protection Officer (if the organisation has appointed one) or another contact person
- the likely consequences of the data breach; and
- any measures that have been taken or are proposed by the controller to address the breach or mitigate the effects of that breach

If a notification is made after the 72 hour period has expired, the data controller must explain the reasons for the delay. The organisation can supply information over time if it is not all available at the time. The regulatory body may require the organisation to notify the public if they consider the breach to be serious enough.

Potentially more complex is the requirement to notify the data subject (the individual) themselves. GDRP states that any communication with the individual must explain "in clear and plain language, the nature of the breach". The notification must include contact details of the organisation involved with the name of the Data Protection Officer if there is one. It must explain the extent and the likely outcome and consequences of the data breach and measures taken or proposed by the controller to address the breach and/or mitigate its effects.

In some situations such as the data having been made unusable by a 3rd party or if it is encrypted , a data subject does not need to be notified, but there is still an obligation for some action by the organisation breached. For example, a public announcement may be considered sufficient by the regulatory authority depending on the exact circumstances and the nature of the unauthorised data exposure.

This is all open to interpretation and flexibility of course, but every data controller ("defined as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal **data** are, or are to be, processed) has a responsibility to assess their own breach situation degree of assessment of the situation. There will inevitably be varying interpretations and assessments as to when a data breach poses a risk and when such risk is sufficiently serious to require notification to the individual data subjects.

In order to avoid any of the doubt, the chance of data breaches occurring should be minimised, of course.

However in order to be prepared, all organisations should ensure that a procedure is defined and that all staff are aware how and to whom, within the organisation, they need to report a data breach. This will ensure that the organisations can determine quickly whether the breach needs to be reported to the authorities and the data subjects.

The ICO recommends that "In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place".

All organisations should have policies in place to assess risk and to be able to demonstrate compliance as a minimum.

Written by Carol Tullo, Senior Consultant of The Trust Bridge

Associate Consultant with The Trust Bridge

Carol Tullo is a Senior Consultant with The Trust Bridge and Legal Counsel. Carol was until July 2017, Director of Information Policy and Services, Controller and Queen's Printer, National Archives, Carol was responsible for providing leadership in information management and policy across government and the wider public sector to improve the way information is managed and exploited to deliver real benefit for those that use and access this valuable resource. As Controller of Her Majesty's Stationery Office, Queen's Printer of Acts of Parliament, Queen's Printer for Scotland, and Government Printer for Northern Ireland, she delivers a range of UK wide official documents.

Penny Heyes is the Co Founder of The Trust Bridge leading a team of highly qualified experts who guide organisations through the processes they needs to ensure that they handle personal data rights and consent in compliance with the General Data Protection Regulation, which comes into force in May 2018. The Trust Bridge came together to offer businesses a unique combination of expertise designed to ensure that they deliver trusted, compliant services to their customers, in the light of the new GDPR regulations coming into force in May 2018

www.thetrustbridge.co.uk

UNITED KINGDOM and EUROPE:
Tel: +44(0) 207 1755 882

USA and CANADA:

Tel: 803 348 000

Solutions and advice you can trust in a data enabled world

 July 2019