GDPR AND NYDFS CYBERSECURITY REGULATIONS

PRIVACY, ETHICAL ISSUES AND REGULATIONS

Sneha Rangari & Cameron Behdani

201810-ITIS-6200-091: ITIS-8200-091-XLSJZ201810_Combined

24th April 2018

Table of Contents:

Introduction:

Cybersecurity is one of the most critical challenges faced by all nations and economies. Many organizations implement technical measures including firewalls, anti-virus software, intrusion detection and prevention systems, encryption, and login passwords. Today's world needs to think beyond technology controls and must attempt to improve cybersecurity through collaborative efforts between government and the private sectors by defining and enforcing stringent cyber laws and regulations. Industry regulators, including banking regulators, have taken notice of the risk from cybersecurity and have either begun or planned to begin to include cybersecurity as an aspect of regulatory examinations. Regulatory updates providing significant restrictions on many current business practices regarding data collection and use as well as reshaping the way organizations across the region approaching data privacy are necessary for the future.

Information at Risk:

There are various types of information which are handled by organization which might include individual's personal information, organizational trade secrets, financial information, etc. Below are types of information at risk:

- Personal Data - Any information relating to an identified or identifiable natural person
- Sensitive Personal Data - Consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
- Trade secrets - A trade secret is a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information not generally known or reasonably ascertainable by others by which a business can obtain an economic advantage over competitors or customers.
- Financial statements - Financial report is a formal record of the financial activities and position of a business, person, or other entity.

Data Protection:

Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes.

Data protection should always be applied to all forms of data, whether it be personal or corporate. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.

Despite of stringent data protection measures, the number of data breaches are increasing on daily basis across the world. Over 1.9 Billion data records were stolen or lost in first half of 2017. Below are some statistics of data breaches:

https://breachlevelindex.com/

GDPR and NYDFS Cybersecurity Regulation:

A **Cybersecurity regulation** comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyberattacks like viruses, worms, Trojan horses, phishing, denial of service (DOS) attacks, unauthorized access (stealing intellectual property or confidential information) and control system attacks.

Implementing these regulations will enhance data security in following ways:

1. Significant restrictions on current business practices regarding data collection and use.
2. Reshaping the way organizations across the region approaching data privacy.
3. More accurate data - New regulations will require data controllers to rectify any identified errors they are told about, it means the accuracy of data stored will be greatly improved.
4. Improved data security - With the scale and sophistication of these attacks growing each day, having a Regulation-compliant framework in place will extend your cyber security practices.
5. Increased alignment with evolving technology - Organization will have to move towards improving its network, endpoint, and application security.
6. Better decision-making – These regulations mandates the right to obtain human intervention, thereby decreasing room for arbitrary decisions.

GDPR:

- The General Data Protection Regulation (GDPR) is focusing on data protection and privacy of all individuals within the European Union.
- It addresses the export of personal data outside the EU.
- The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
- It will replace the 1995 Data Protection Directive (Directive 95/46/EC) - A set of principles in order to keep someone's data accurate, safe, secure and lawful.
- It was adopted on 27 April 2016. It becomes enforceable from 25 May 2018, after a two-year transition period.
- There are total 173 requirements as well as 11 Chapters consisting of 99 Articles.

GDPR Key Changes:

Although the key principles of data privacy still hold true to the previous EU Data Protection directive, GDPR come up with many significant changes to the regulatory policies. It is essential to understand changes proposed in GDPR and impact it would have on business. This is briefly explained as below

- Increased Territorial Scope (extra-territorial applicability):

GDPR applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'.

- Penalties:

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment.

- Consent:

GDPR mandates consent shall be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

- Right to Access:

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

- Right to be Forgotten:

This is also known as Data Erasure. The right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

- Data Portability:

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

- Data Protection Officers:

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences.

- Breach Notification:

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.

Rights of Data Subjects Under GDPR:

The GDPR provides the following rights for individuals:

- Right to be informed:

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

- Right of access:

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

- Right to rectification:

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. You have one calendar month to respond to a request.

- Right to erasure:

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. You have one month to respond to a request.

- Right to restrict processing:

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, you are permitted to store the personal data, but not use it.

- Right to data portability:

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- Right to object:

Individuals have the right to object to:

    - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

- direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

Rights related to automated decision making including profiling:

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement); and
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Case Study:

Equifax Breach Affects 143M: If GDPR Were in Effect, What Would Be the Impact?

- Notification obligations for security breaches that affect U.S. residents are governed by a patch worked set of state laws.
- The timing of the notification varies from state to state with some requiring that notification be made in the "most expeditious time possible," while others set forth a specific timeframe such as within 30, 45, or 60 days.
- While the majority of the affected individuals appear to be U.S. residents, Equifax stated that some Canadian and UK residents were also affected.
- Given Equifax's statement, the notification obligations under GDPR would apply, even post-Brexit, as evidenced by a recent statement of intent maintaining that the United Kingdom will adopt the GDPR once it leaves the EU.
- Under the GDPR, in the event of a personal data breach, data controllers must notify the supervisory authority "without undue delay and, where feasible, *not later than* 72 hours after having become aware of it."
- If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay. A notification to the authority must at least: 1) describe the nature of the personal data breach, including the number and categories of data subject and personal data records affected, 2) provide the data protection officer's contact information, 3) describe the likely consequences of the personal data breach, and 4) describe how the controller proposes to address the breach, including any mitigation efforts.
- If it is not possible to provide the information at the same time, the information may be provided in phases "without undue further delay."
- According to Equifax's notification to individuals, it learned of the event on July 29, 2017. If GDPR were in effect, notification would have been required much earlier than September 7, 2017. Non-compliance with the notification requirements could lead to an administrative fine of up to 10 million Euros or up to two percent of the total worldwide annual turnover.

Preparing for the General Data Protection Regulation (GDPR):

This checklist from the U.K. Information Commissioner's Office highlights 12 steps you can take to begin preparing now for the GDPR, which will come into effect in 2018.

Awareness:

You should make sure that decision makers and key people in your organization are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Information you hold:

You should document what personal data you hold, where it came from and who you share it with. You may need to organize an information audit. You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Communicating privacy information:

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Individuals' rights:

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Subject access requests:

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Lawful basis for processing personal data:

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Consent:

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Children:

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

Data breaches:

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Data Protection by Design and Data Protection Impact Assessments:

You should familiarize yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organization.

Data Protection Officers:

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organization's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

International:

If your organization operates in more than one EU member state (i.e. you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Impacts of GDPR:

1) **Legal and Compliance**- Require proactive, robust privacy governance, requiring organizations to review how they write privacy policies, to make these easier to understand.
2) **Technology**- Security breaches will have to be notified to regulators within 72 hours, organizations will be expected to look more into data masking, pseudo-anonymization and encryption.
3) **Data**- Better grasp of what data is collected and where it is stored will make it easier to comply with new data subject rights – rights to have data deleted and to have it ported to other organizations.

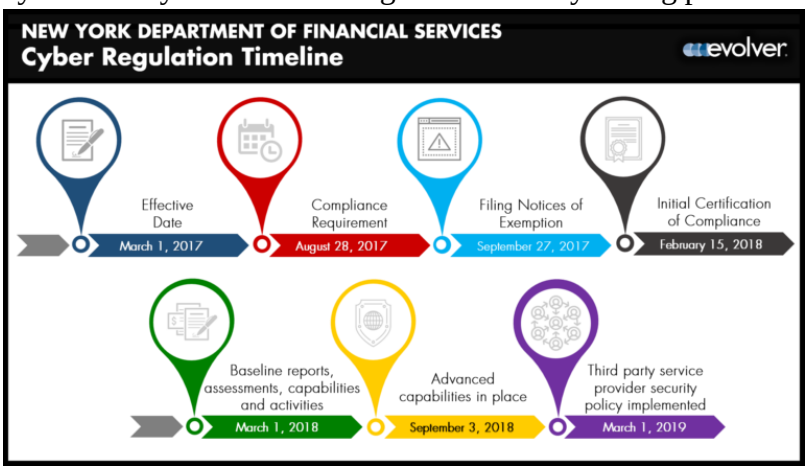
Limitations of GDPR:

1) The requirement to have a Data Protection Office (DPO) may add an administrative burden

2) Language and staffing challenges for Data Protection Authorities (DPAs)
3) Lack of privacy experts
4) Cost: Update internal policies, appoint a Data Protection Officer and ensure that products all take a privacy first approach in very design.
5) New Software that offers Data Loss Prevention or data classification features should be implemented.
6) Massive fines which companies found to be non-compliant.

New York Dept. of Financial Services Cybersecurity Regulations:

- The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a new set of regulations from the NY Department of Financial Services (NYDFS) that places new cybersecurity requirements on all covered financial institutions.
- The rules were released on February 16th, 2017 after two rounds of feedback from industry and the public. Covered institutions must adhere to many of the new requirements by as early as August 28, 2017.
- It is one of the first instances of Cybersecurity regulation in the United States. It mainly focused and designed to protect consumers' private data specifically financial one.
- It assesses confidentiality, integrity and availability of financial information systems. It helps to identify material cyber-risks related to financial data.
- It also helps to propose steps to remediate inadequacies identified. It includes material cybersecurity events involving covered entity during period addressed in report.



NYDFS Cybersecurity Regulations Key Changes:

Early Alerts:

Notify NYDFS, no later than 72 hours from a determination that a cybersecurity event has occurred, if that event either (1) requires the company to provide notice to any government body, self-regulatory agency or any other supervisory body; or (2) has a reasonable likelihood of materially harming any material part of the normal operations of the company. An attack may constitute a reportable cybersecurity event even if the attack is not successful.

Annual Cybersecurity Report submitted by CEO of affected companies:

Submit report to Superintendent by Feb 15 attesting to compliance with requirements, signed by Chair of Board or senior officer to best of knowledge

- Retain supporting records, schedules for 5 years
- Material improvements required for areas, systems, etc. Document identification and remedial efforts and retain for examination
- Be available for inspection

Cybersecurity personnel and training:

Utilize qualified cybersecurity personnel (who may be employed by the company or a third-party service provider) to manage cybersecurity risks and to perform core cybersecurity functions; provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

Risk assessment:

- Conduct and document a periodic risk assessment that considers the particular risks of the company's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized, and the availability and effectiveness of controls to protect nonpublic information and information systems.
- The risk assessment must be carried out in accordance with written policies and procedures that include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats;
(2) criteria for the assessment of the confidentiality, integrity, security and availability of the company's information systems and nonpublic information, including the adequacy of existing controls in the context of identified risks; and
(3) requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks.

Data retention requirements:

Earlier data of financial related things used to get retained for five years, but according to NYDFS data retention policy is reduced from five to three years. Thus keeping the information retained for shorter period will reduced the risk.

Newly defined limited exemptions:

Now include the gross annual revenue and the number of employees of a Covered Entity's affiliates in New York.

Clarified exemption rules:

Exemption rules clarified for companies regulated under the insurance laws of New York.

Impacts of NYDFS-CR:

The Cybersecurity Regulations can impact businesses globally, even if they do not do business in New York:

If your business is a bank, trust, budget planner, check casher, credit union, money transmitter, licensed lender, or mortgage broker covered by New York's Banking Law, Insurance Law, or Financial Service Law, you most likely need to comply. The regulations apply even if you only do business in New York but have no physical presence.

Apply directly to any Covered Entity:

The regulation is expected to impact a large number of businesses, to include those directly supervised by the NYDFS and many of their third party service providers and third party application providers. Whether or not a company is headquartered in New York, the Rules apply to all entities subject to the authority of NYDFS under New York banking, insurance and financial services law ("Covered Entities").

Some entities are exempt from parts of the Rule (including many smaller companies, although even they have compliance and filing requirements), and some insurance and reinsurance entities that are subject to other New York regulations may be exempt from this Rule entirely. These regulations will not apply to national banks and federal branches of foreign banks but will apply to New York-licensed lenders and branches of foreign banks. Covered companies will also need to consider the application of any federal cybersecurity guidelines.

Apply indirectly to Third Party Service Provider(s):

Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible 7 to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity.

Limitations of NYDFS-CR:

- Organizations with less than 10 employees and independent contractors are considered exempt under the enacted version of the regulation.
    - Exemption from certain sections is available to Covered Entities with:
    - Fewer than 10 employees, including independent contractors, of the CE or its Affiliates located in NY or responsible for business of the CE;
    - Less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the CE and its Affiliates; or
    - Less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates.
- Small and medium-sized companies can rely on third party service providers to meet many of the regulation requirements.

Our Thoughts and Conclusions:

- Regulations are going to help the legal system catch up with some of the technology that's permeated our lives over the last couple of decades.
- These regulations will act as a baseline and pave the way for future cybersecurity regulations
- Improved Business Reputation- With the threat of attack so high, being certified as GDPR complaint is going to be a major plus in marketing terms, boosting your business's reputation as secure in the eyes of potential customers.

References

1. *https://www.dfs.ny.gov/about/cybersecurity.htm*
2. *https://www.bitsighttech.com/blog/nydfs-cybersecurity*
3. *https://www.eugdpr.org/*
4. *https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-gdpr-vision-approach.pdf*
5. *https://www.inma.org/blogs/ideas/post.cfm/pros-cons-of-eu-s-general-data-protection-regulation-for-publishers*
6. *https://www.rapid7.com/fundamentals/nydfs-cybersecurity-regulation/*
7. *https://digitalguardian.com/blog/nydfs-clarifies-questions-around-cybersecurity-regulation-rule*