Three Key Risks and Opportunities of GDPR

At a Glance

This white paper explores three key risks and opportunities that information security and risk management professionals should consider when developing an overall GDPR strategy.

While some of the threats posed by GDPR are obvious, such as the fines for non-compliance, there are some other noteworthy risks that should also be taken into account. These include being held liable for non-compliance of partners and vendors and the trend of GDPR-like legislation spreading to other major economic zones across the globe.

On the other hand, a well-rounded GDPR strategy should also take into account that there are a number of opportunities that can be associated with GDPR as well. In fact, some risks can be turned around and made into opportunities. Keeping both risks and opportunities in mind is necessary to create a balanced and informed strategy.

RISKS

Fines for non-compliance

At the top of the list is the most obvious and widely publicized GDPR-related risk, the financial penalties for non-compliance, which can be as high as 20 million EUR or 4% of global annual revenue from the previous financial year, whichever is higher. These penalties are intentionally steep and are, among other things, what truly sets GDPR apart from the European Commission's previous data protection standard, the 1995 Data Protection Directive.

Despite the two year phase-in period from 24 May 2016 to 25 May 2018, many organizations are still non-compliant. According to a study released by iWelcome in June of 2018[1], 66.3% of European companies were still uncompliant, with Germany having the lowest rate of non-compliance at 34.8%. According to the November 2017 GDPR pulse survey by PwC[2], 28% of US companies had only just begun to prepare for GDPR compliance while 10% responded that they were already prepared. Despite such high rates of non-compliance, the EU Commission has not issued any GDPR-related fines to date.

Just weeks before the deadline on 25 May 2018, 66.3% of European companies were still not compliant with GDPR[1].

How the amount of the fine is determined
20 million EUR or 4% of global annual revenue is the absolute maximum penalty. However, according to Article 83 (2) the amount of the fine is determined on a case by case basis and should be proportional to the gravity of the infringement. A number of factors are taken into consideration, including the nature and duration of the infringement, the number of data subjects affected, the type of personal data, intent, adherence to approved codes of conduct and certifications, and any efforts taken to minimize the damage to data subjects.

Furthermore, the maximum penalty of 20 million EUR or 4% of global annual revenue only applies to violations of certain provisions enumerated in Article 58, Paragraph 4:

- Basic principles of processing, such as lawfulness and consent (Articles 5, 6, 7 and 9)
- The rights of data subjects, such as the right to be forgotten (Articles 12 to 22)
- Transfers of personal data to third countries or international organizations (Articles 44 to 49)
- Obligations pursuant to member state law adopted under Chapter IX
- Failure to comply with an order to limit or suspend processing pursuant to Article 58 (2)
- Failure to provide access to the supervisory authority pursuant to Article 58 (1)

The above violations generally deal directly with the privacy of data subjects, which is the main focus of GDPR. A lesser maximum fine of 10 million EUR or 2% of global annual turnover applies to infringements described in Article 58, Paragraphs 5 & 6:

- Obligations of controller and processor (Articles 8, 11, 25-39, 42, and 43)
- Obligations of the certification body (Articles 42 and 43)
- Obligations of monitoring body (Articles 41(4))

These fines are more related to administrative non-compliance, which is treated less severely than direct violations of the privacy of data subjects.

1 https://www.iwelcome.com/category/news/gdpr-research-update-66.3-percent-european-organisations-not-compliant
2 https://www.pwc.com/us/en/services/consulting/cybersecurity/general-data-protection-regulation/pulse-survey-insights.html

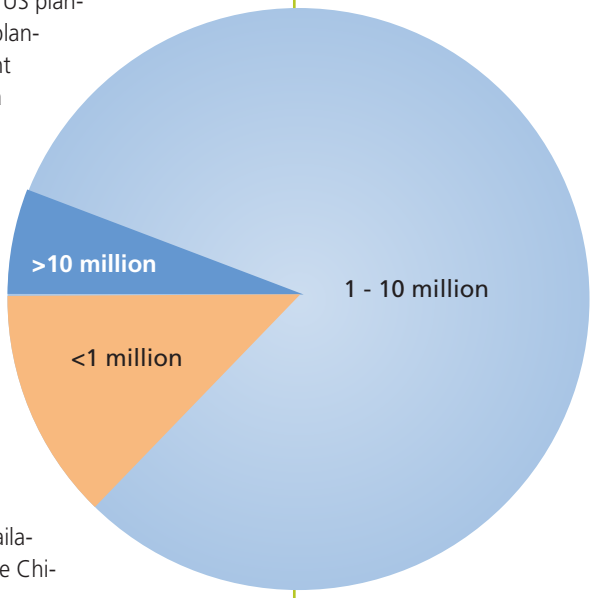
RISKS
Fines for non-compliance

How these potential fines affect the business

When faced with the risk of penalties this high, organizations have no choice but to take the regulation seriously. If the penalties were lower, companies might decide that they would be better off ignoring the provisions of the regulation and simply paying the fines. There are two major economic factors that the penalties have to outweigh: the total cost of compliance and the value lost due to the limitations on data analysis set by the regulation. For organizations whose entire business model hinges on processing and brokering personal data, the latter may be even more painful than the former.

According to a GDPR pulse survey from PwC[3], 77% of companies in the US planned to spend upwards of 1 million USD on GDPR compliance, with 9% planning to spend 10 million USD or more. If the EU market plays a significant role in an organization's revenue, then spending 1 million USD to avoid a potential payout of 22.8 million USD[4] is an easy decision to make.

77% of US companies were planning to spend over $1 million on GDPR compliance



PwC GDPR Preparedness Pulse Survey December 2016[3]

Similar regulations catching on elsewhere

The GDPR is extremely broad in its scope because it applies to all organizations who process data of EU residents, even if those organizations are based outside of the EU. To avoid both the potential fines and costs of compliance described above, some non-EU companies have opted to withdraw from the EU market entirely. For example, as of November 2018, six months after GDPR came into effect, every US-based online newspaper managed by Tribune Publishing Company has been routing all traffic from EU IP addresses to pages that say something to the effect of "our website is currently unavailable in most European countries". This includes the Los Angeles Times, the Chicago Tribune, Long Island Newsday, and many more.

For companies that only had an inconsequential amount of business and traffic coming from the EU, such as a US-based newspaper, it might make economic sense to skip GDPR compliance and simply withdraw from the EU market. While this strategy might make sense in the short term, it may not be sustainable in the long term. Major economic centers across the globe are beginning to introduce similar data privacy and protection legislation, including Brazil, Australia, Japan, South Korea, and the US States of California and New York, among others. As this kind of legislation begins to appear in more parts of the world, it will become more and more difficult to find refuge in a "GDPR-free" market. Eventually, organizations will have no choice but to comply with either GDPR or similar regulations.

3 https://www.pwc.com/us/en/services/consulting/library/gdpr-readiness.html
4 According to XE.com, as of 6 November 2018, 1 EUR = 1.14 USD.

RISKS
Similar regulations catching on elsewhere

Brazil

Brazil's Lei Geral de Proteçao de Dados (LGPD) was modelled directly after GDPR and is nearly identical in terms of scope, applicability and financial penalties for non-compliance. Companies wishing to do business with Latin America's largest economy will have to comply with LGPD by February 2020 or be subject to maximum fines of 50 million BRL (approximately 11.8 million EUR[5]).
The full text (in Portuguese) of the LGPD can be found on the official website of the President of Brazil[6].

Japan

In July 2018, the European Commission published a press release[7] announcing the "reciprocal adequacy" of data protection systems between the European Union and Japan. In order to qualify for the adequacy decision from the Commission, Japan has committed to implementing additional safeguards to protect individuals in the EU whose data is transferred to Japan. These additional measures include stronger protection of sensitive data, stricter conditions under which EU data be transferred via Japan to another third country, the rights to access and rectification for data subjects, as well as a complaint-handling mechanism for Europeans inquiring about access to their data by Japanese public authorities.

USA: State of California

California's Consumer Privacy Act of 2018 (CaCPA) contains many provisions reminiscent of GDPR, specifically those regarding consumer privacy. According to CaCPA, residents of California have the right to know what personal information is collected about them, whether that information is being sold and to whom, the option to forbid the sale of their personal information, the ability to access and amend their personal information, and the right to equal service and price even if they exercise their privacy rights. CaCPA applies to larger organizations that process personal information of California residents, regardless of whether that organization is physically based in California, and non-compliance can carry penalties of 7,500 USD per intentional violation and 2,500 USD per unintentional violation. Penalties for failure to disclose covered data breaches are determined by 100 to 750 USD per affected California resident.
The full text of the California Consumer Privacy Act of 2018 can be found on the California State Legislature website.[8]

USA: State of New York

New York State's Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500) only applies to financial organizations with branches in New York, but the requirements for treatment of "Nonpublic Information" overlaps in many ways with GDPR requirements for handling personal data, including encryption of data in motion and at rest, data breach notifications, appointment of a CISO (analogous to a DPO under GDPR), data retention limits, etc. Financial institutions in New York State have to comply with 23 NYCRR 500 or face fines of up to 250,000 USD or revocation of their licenses.
The full text of 23 NYCRR 500 can be found on the New York State Governor's website.[9]

Australia

The Office of the Australian Information Commissioner (OAIC) recently updated Australia's Privacy Act with the Privacy Amendment (Notifiable Data Breaches) Bill, which came into effect in February 2018. Organizations with an annual turnover of over 3 million AUD will have to disclose data breaches that pose a "real risk of serious harm" within 30 days of their discovery or face fines of up to 1.8 million AUD.
The full text of the NDB is available on the Australian Government's Federal Register of Legislation website.[10]

5 According to XE.com, as of 5 November 2018, 1 EUR = 4.22 BRL.
6 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm
7 http://europa.eu/rapid/press-release_IP-18-4501_en.htm
8 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
9 https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
10 https://www.legislation.gov.au/Details/C2016B00173

RISKS

Liability for suppliers and vendors that handle personal data

The third key risk of GDPR is that organizations can also be held liable for the indiscretion of vendors and suppliers who process or handle personal data on their behalf. This includes data of employees as well as customers and clients. These requirements are described in GDPR Chapter IV, Controller and Processor. As defined in Article 4, in a situation where one organization hires another to process data on their behalf, the subcontractor is considered the processor and the company that hires them is the controller.

Organizations must properly vet new suppliers and vendors and, where applicable, assess and renegotiate terms with existing vendors and suppliers. There are a number of steps organizations must take to avoid penalties:

- **Update existing contracts as well as templates for new contracts:**
  - > **Define personal data, processor, and controller according to Article 4**
  - > **Controller must clearly delineate processor's scope of processing in accordance with Article 28**
- **Conduct compliance audits of processors regarding data protection and request documentation of technology, processes and procedures**
- **Coordinate with processor to determine data breach notification procedures**
- **Compliance officers and vendor management leaders should review all new initiatives to subcontract data processing**

According to Article 83, violations of these requirements are subject to a maximum fine of 2% of global annual revenue or 10 million EUR, whichever is higher. In the past, selection of IT vendors was determined first by cost and second by security, however given the potential for such high fines, cost can no longer be judged without considering security. This makes GDPR compliance a non-negotiable requirement when selecting IT service providers.

OPPORTUNITIES

Organizations wishing to tackle GDPR compliance should not view it as just another regulatory burden and should consider that there are a number of opportunities that the GDPR affords.

The best way to turn GDPR into an opportunity is to leverage GDPR requirements to the organization's advantage.

Here are the top 3 ways this can be achieved at any given organization:

More meaningful and productive engagement with potential customers

In order to comply with the GDPR, organizations must have explicit consent to store and process personal data. On the surface, this may seem like a threat to the marketing and sales pipeline as it reduces the addressable audience, but it has an upside. Having a smaller list of contacts who have all indicated they would like to hear from the company will greatly increase the value of each individual contact.

In the days and weeks leading up to 25 May 2018, many people, especially those who reside in the EU, received emails from a range of companies asking whether they consented to receiving marketing emails in the future. These emails were all part of permission pass campaigns intended to cleanse companies' contact databases of recipients who may not have consented to receive communications from the company. This was done to comply with the requirement of gaining explicit consent before contacting a data subject. Contacts who did not respond to the permission pass campaign emails after 25 May had to be treated as ineligible for further communications. This shrunk companies' addressable audiences immensely, in many instances by more than half.[11]

In fact, this has a positive effect for both companies and costumers. Customers will receive less spam and grey mail, and companies will spend less time and resources on individuals who are not interested in their products and services, allowing them to focus on contacts who have demonstrated a genuine interest. As a result, marketers will see an increase in the rate of engagement with their messaging. If a marketing email is sent to only 100 recipients but half are interacted with, that should be seen as more valuable than sending to 200 recipients but only getting interactions.

The goal of marketers will no longer be about addressing the highest number of contacts possible and instead will shift towards addressing individuals who are most likely to become customers. As quality takes priority over quantity, the KPI of number of recipients will become secondary to the percentage of recipients who open the message and click on a call to action.

As marketing begins to focus more on delivering higher quality leads rather than the highest possible volume of leads, lead management will become more efficient. Sales teams will be delivered higher quality leads with the potential to close at a higher rate than in the past.

11 https://www.zdnet.com/article/gdpr-whats-really-changed-so-far/

Framework for common sense data security

GDPR provides a framework for comprehensive data security that includes standards for breach management, data protection, vendor management, data minimization and so on. On top of that, the fines for non-compliance provide an impetus to implement these policies sooner rather than later.

Data protection by design and by default

GDPR is heavily influenced by the concept of "Privacy by Design", hence the title of Article 25 'Data protection by design and by default'. As described by Ann Cavoukian, former Information & Privacy Commissioner of Ontario Canada, Privacy by Design has seven foundational principles:[12]

1. Proactive not reactive; preventative not remedial

This principle is reflected in GDPR via requirements such as data breach impact assessments and pseudonymisation of data. They ensure that organizations and the data they manage are protected and response plans are defined before an incident occurs.

2. Privacy as the default setting

This principle influenced the way companies conducted permission pass campaigns and designed their cookie consent banners. If a recipient did not respond to the consent to contact email, then it should have been assumed that they did not wish to be contacted again in the future. Furthermore, non-essential tracking cookies would be disabled by default, meaning that users would have to opt-in to non-essential cookies rather than opt-out.

3. Privacy embedded into design

Privacy embedded into design means IT systems and business processes are developed with privacy in mind and privacy is protected without reducing functionality. This is prerequisite to all subsequent principles of Privacy by Design.

4. Full functionality – positive-sum, not zero-sum

Privacy should result in a win-win situation. As described in the first opportunity section "more meaningful and productive engagement with potential customers", privacy can be advantageous to both sides of the equation. On the one hand, marketing and sales can focus contacts who have a much greater chance of conversion while consumers are only contacted by companies whose products and services they are genuinely interested in.

5. End-to-end security – full lifecycle protection

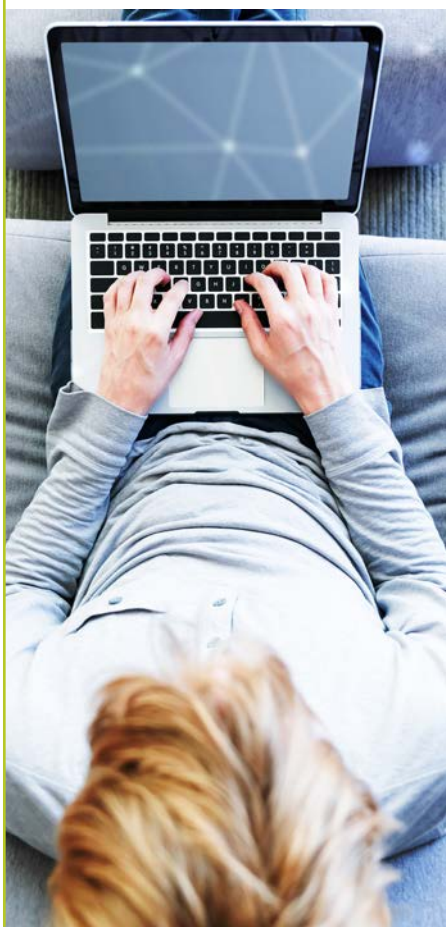
Full lifecycle protection for personal data means protecting the data whether it is in rest or in motion (Article 32), only retaining data for clearly defined purposes and deleting it when it is no longer useful (Article 25) or when the data subject requests it be deleted (Article 17).

6. Visibility and transparency – keep it open

In the interest of visibility and transparency, many companies updated their privacy policies to be GDPR compliant. These updates included, among other things, detailed lists of all tracking cookies that indicate where the cookies came from, what data they collect, how long the data is kept, and for what purpose.

7. Respect for user privacy – keep it user-centric

All of the above principles form a foundation for user-centricity which is a core tenet of data privacy and the rights of data subjects.



12 https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Impetus for proactive investment in data protection

Risk and security experts are more than aware of the principles of privacy by design and the array of threats that face enterprise data, yet they often struggle to secure the budget that is required to properly secure sensitive data in their organization. The unfortunate reality is that many companies do not take the threat of a data breach seriously until after one has taken place, whether by malicious actors, negligence, or both. The reason for this is the probability of a breach being fairly low coupled with the potential for only minor damage being done to the company's reputation. Most companies who have suffered even major data breaches in recent years have recovered mostly unscathed. The external costs to the individuals whose data was compromised was not taken into account.

GDPR was drafted with these external costs in mind, which is why the fines are partially influenced by the number of data subjects affected. With the potential for such high fines, the risk factor of not preparing for data breaches has become significantly higher, perhaps high enough to motivate pro-active investment in adequate data protection.

Uniform data privacy and protection standards for international business

The risk described above in "similar regulations catching on elsewhere" can also be viewed as an opportunity. The more regulations from different countries overlap, the easier it becomes to manage international compliance.

Across the EU

From its inception, the EU was designed to facilitate commerce across the continent. GDPR was drafted in that same spirit and offers companies the opportunity to unify their data privacy policies instead of having to fumble with disparate laws and standards that vary from country to country. Companies that are GDPR compliant will therefore have access to an entire economic zone which, according to the World Bank, had a combined nominal GDP of 17 trillion USD in 2017, larger than that of China and only slightly behind the United States.

Globally

As mentioned above, GDPR overlaps with certain parts of data privacy standards from other parts of the world as well, including Australia, Brazil, Japan and the US States of California and New York. It also overlaps with PCI DSS to a large extent. If the trend continues, these standards will overlap with the GDPR more and more. Achieving GDPR compliance now will put non-EU companies ahead of the game, because even if they are not focused on the EU market, similar standards are likely to appear in their home markets sooner or later.

Conclusion

GDPR and its penalties for non-compliance are a tremendous source of risk for organizations that process personal data of EU residents. For many organizations, a 20 million EUR fine could even pose an existential threat, which may motivate some to abandon the EU market entirely. However, as described above, running away from the problem is only a quick fix which will not be viable in the long term as similar legislation emerges across the globe. Sooner or later it will become necessary to implement a comprehensive data protection strategy, regardless of the target market. The best strategy for tackling GDPR compliance will be a balanced approach that takes both the risks and opportunities into account. One of the biggest opportunities may be leveraging the investment into GDPR compliance to cover compliance with similar regulations in other parts of the world.

A common denominator in privacy regulations around the world is that sensitive data must be protected because **data protection is a fundamental part of data privacy**. We recommend a pro-active, privacy by design approach that includes appropriate technology to ensure that sensitive data is protected end-to-end from the moment it is collected, all the while it is being used, until finally it is discarded. Smart technologies, such as data-centric security and tokenization, can keep the data protected at all times, regardless of whether it's in storage, in use, or in motion.

data protection is a fundamental part of data privacy

This document is not intended as legal advice or to recommend any specific course of action. Always consult with your legal counsel when determining the legally binding obligations of any regulation or contract.