THE GENERAL DATA PROTECTION REGULATION: SHOULD IT MATTER TO ME AND HOW CAN TECHNOLOGY HELP?

An Industry Perspective Report brought to you by ASG Technologies and FIMA

This report is based on recommendations made by industry experts who participated in the General Data Protection Regulation webinar. In addition, it includes benchmark data gathered on-site at the FIMA conference on May 18, 2017.

asg technologies™ FIMA Financial Information Management WBR DIGITAL

WEBINAR BACKGROUND INFO

In the Spring of 2017, ASG and the FIMA conference series partnered to produce a webinar focused on the questions that have arisen since the EU's adoption of the General Data Protection Regulation (GDPR). The GDPR is intended to strengthen and unify data protection for all individuals within the European Union and could have broad implications for companies and organizations operating in the zone.

This report uncovers the answers to common concerns, as identified by industry experts, and includes recommendations on complying with this new regulation.

Robert Perry
Vice President of Product Management
ASG Technologies

Anne Cavoukian, Ph.D.
Executive Director
Privacy and Big Data Institute
Ryerson University

HAVE BUSINESSES MADE ANY PROGRESS COMPLYING WITH THE GDPR?

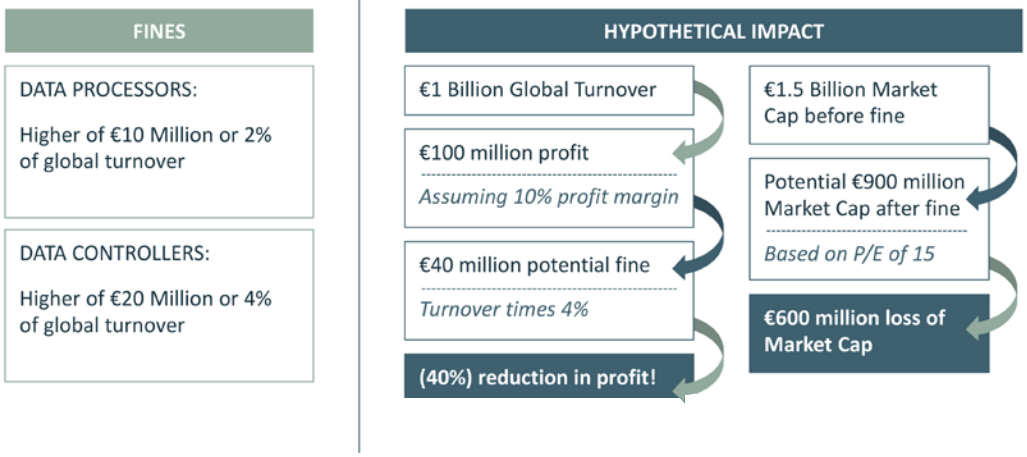
If you're a company on the outside that collects data on EU individuals, it affects you as well.

Robert Perry
Vice President of Product Management
ASG Technologies

Robert Perry: The GDPR goes into enforcement May 25, 2018. It gives the control of information back to the individual while giving the controllers and processors specific responsibilities they must abide by. This regulation has global reach. It is a European Union regulation that affects and protects the people who reside within the EU, but if you're an organization on the outside that collects data on EU individuals, it affects you as well.

Under the U.K.'s data protection law, there have already been fines levied in the tens of thousands of pounds. In terms of business, this is a moderate amount of money, but this will not be the case under the GDPR. The fines under the GDPR can be millions of euros to up to 4% of your global turnover or global revenue, which has a larger impact on your company. For example, if you had a profit of 100 million euros you could lose 40 million of that amount.

FINES HAVE SIGNIFICANT FINANCIAL IMPACT



We've seen surveys where 45% of senior management see the size of these fines as their main concern. People aren't sure about the impact and how to go forward. Privacy by Design is one of those areas of confusion. Also, according to these surveys, half of companies have not applied a budget to ready themselves for GDPR. Within that half, some companies believe they can manage within their current budgets. A lot of respondents have set aside specific budgets, designated specific people for the task, and put processes in place.

85% have hired a data protection officer. For many companies, it is a requirement under the GDPR that they have this person in place. It doesn't just apply to businesses, it applies to all types of organizations that collect personal data. The survey found that only one-third of organizations' processes are compliant today. Two-thirds of their processes were not compliant.

COMPANIES ARE EXPRESSING CONCERN BUT ACTING SLOWLY

41% Believe data security and breach notification will have high impact on organization

Identified areas of confusion:

1. Legitimate interest
2. Privacy by design and pseudonymization
3. Privacy impact assessment and risk

45% Senior management with concerns about enhanced sanctions

49% **Yet many organizations have not set budgets**

In descision process about budgeting for compliance

Source: Organisational Readiness for the European Union General Data Protection Regulation (GDPR), Center for Information Policy Leadership and Avepoint.

PROGRESS IS BEING MADE, WITH MORE TO BE DONE

Requirement for DPO is being met

85% Have appointed Data Privacy Officer

Many companies perform privacy impact assessments (PIA) already

55% Conduct PIA in situations identified in GDPR...

However, few companoes are currently gaining consent in compliance with GDPR

1/3 Share seemingly in compliance with enhanced consent requirements

Yet few use systematic, organized approach

25% Use automated system (in-house or commercial)

36% Have procedure or framework to identify and classify risk to individuals

Source: Organisational Readiness for the European Union General Data Protection Regulation (GDPR), Center for Information Policy Leadership and Avepoint.

About one-third have reviewed their processes and are making a change, a third have reallocated budget, and a third replied "somewhat" in that they must have a lot to do or perhaps have a team studying what they need to do for the GDPR. Nobody replied that they hadn't started and that's a great finding, which shows that everyone is taking this seriously.

HOW CAN YOU BECOME COMPLIANT?

Compliance is maintained when you only collect data you need, you gain consent, define the use of data and maintain its quality, you process requests to update the data, you track what data you have, and you delete it when no longer needed.

Robert Perry
Vice President of Product Management
ASG Technologies

FOUR STAGES FOR COMPLYING WITH GDPR

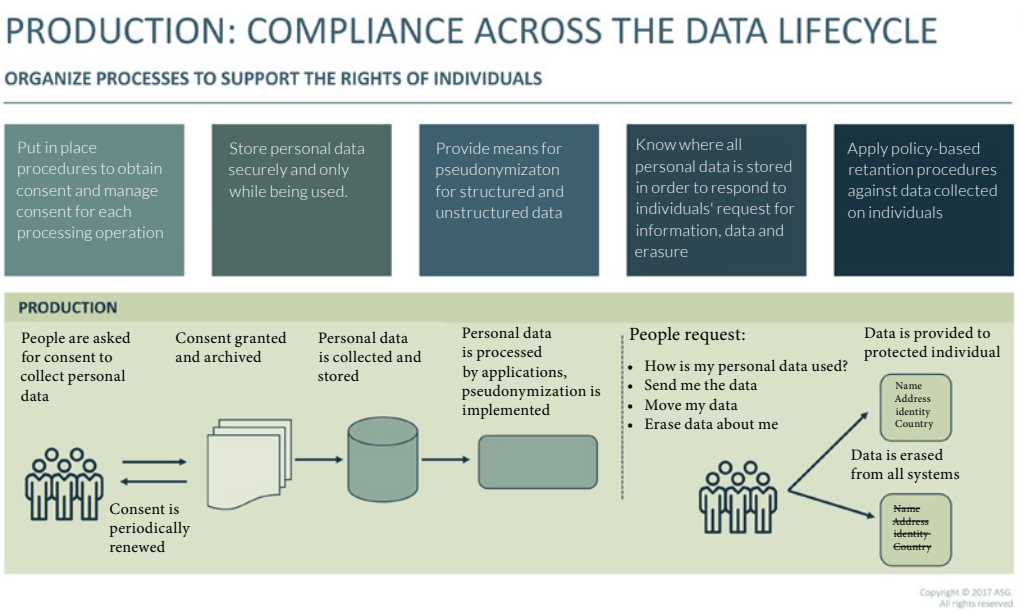
HAVE YOU STARTED?

PREPARATION	Map data and content estates, business processes, data flows that involve personally identifiable data (PID).
PRODUCTION	Operate business processes, handle PID within regulations, respond to data requests from subject (erasure, portability, information), notify of data breach.
GOVERNANCE	Review new processing activities, assure compliance, respond to audits, set internal standards.
REPORTING	Provide reports that provide management view of PID usage, present issues and actions via dashboard and reports. Prove knowledge of data proessed and how it is used. You can also make a Data Lineage report to show where the data comes from, how it is transformed and used throughout the organization while also identifying unused data and having it removed.

Robert Perry: There are four stages in becoming compliant. First, prepare: Understand the situation along with what kind of data you have and how it's being used. Second is the production process: How you assure your processes comply and that you're doing what you need to as you move forward. Third, governance: How you are watching and assuring that you remain vigilant in keeping compliant. Fourth, reporting: Putting reports in place so you can see what data and processes you have while also being ready in case authorities need to ask these questions.

First, the preparation process. A good starting point is getting a handle on the data collected in the past along with what you do with it and whether you should have it. You need to understand what is currently in place before you can start making changes to move forward. There are some important questions to ask: What personal information is being stored? How did I obtain it? Do I have the correct consent for it? Why was it collected? What processing is applied? Is unused personal information being stored?

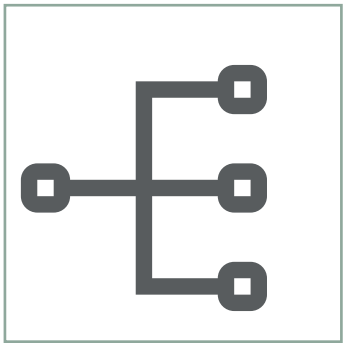
The production process is about compliance across the lifecycle. To remain compliant, you must show how you protect that data and use it only for the means of why it was collected. The individual can request what data you have, how you are using it, that you move it to another processor, or have it erased. You need a means to respond to all those requests. This is where a robust content management system can help.



Next is providing a way of assuring you remain compliant. This is governance. It involves educating your organization so they understand the requirements, but also watching and assuring that you maintain compliance. Compliance is maintained when you only collect data you need, you gather consent, you have appropriate use, you maintain its quality, you process requests to update the data, you track what data you have, and you delete it when no longer needed. Another important part of the governance process is to be ready for audit.

Data Protection Impact Assessments are an ongoing way of assuring you are thinking about privacy and the protection of information when defining new processes. 55% of organizations seem to be doing some level of impact analysis, but the automation is not there. One way that data intelligence products can help with this is by starting from the bottom. Your data can be mapped and viewed through a browser so you and anyone in the organization who has access rights can understand the entire process.

Finally, reporting. It's important to have reports for yourself and the organization but this is also important for audits. Our systems provide the ability to create a Data Inventory Report of all your protected data and show where it is stored and how it is used. You can also make a Data Lineage report to show where the data comes from, how it is transformed and used throughout the organization while also identifying unused data and having
it removed.



WHAT IS THE CURRENT REGULATORY ENVIRONMENT AROUND PRIVACY?

> ***Privacy is about personal control.*** *It's about having control over the use of your personal information. That's why the notion of user control is critical. It reflects the ability to exercise the freedom of choice.*

Anne Cavoukian, Ph.D.
Executive Director
Privacy and Big Data Institute
Ryerson University

Dr. Anne Cavoukian: Privacy is not about secrecy and not about having something to hide. Privacy is about control. I want to make this clear: privacy is about personal control. It's about having control over the use of your personal information. That's why the notion of user control is critical. It reflects the ability to exercise the freedom of choice. You have to be the one to make the determinations as to whether you want your information used for a particular context or not.

Privacy by Design is something I developed in the late '90s. It really took off after 9/11 and then it was adopted as an international standard by the international community of privacy commissioners and data protection authorities in 2010. I introduced a resolution that year on Privacy by Design, which we needed to complement regulatory compliance. We needed something like the medical model of prevention: a proactive way to protect privacy, identify the risks and address them such that you could try to prevent privacy harms from arising. The majority of privacy breaches were remaining largely unknown, unchallenged, and unregulated.

This was unacceptable to us. We needed something that came at the front end of regulatory compliance. Regulation after the fact was no longer sustainable. Privacy forms the foundation of our freedom.

There are seven foundational principles of Privacy by Design.

The first foundational principle is the need to be proactive and prevent harms from arising.

The second foundational principle is that privacy is the default setting. Every survey that has come out in the last two years has shown concern is at an all-time high.

Privacy as a default only allows information to be used for the proposed purpose. Consumers are given privacy assurance right from the outset. They will reward you with their repeat business, loyalty, trust, and this will attract new opportunities.

The third foundational principle speaks for itself. If privacy is formed as part of the design of your operations, then it's not an afterthought but an essential component.

The fourth foundational principle is that it's all about positive-sum, not zero-sum. The world today operates in a zero-sum model. You have to be innovative to achieve positive-sum results, but it is eminently doable.

The sixth foundational principle is visibility and transparency. You as a company may have control over your customers' information, but the data belongs to the individual from which you received that data. This transparency works in your benefit because they are in the best position to correct any faulty information.

The last principle: respect for the user. When you keep it user-centric, the rest just flows seamlessly. You can do both privacy and security, privacy and data analytics, and privacy and marketing. Privacy is not anti-marketing; it's pro-choice.

WHAT DOES THE GDPR MEAN FOR BUSINESS IN THE EU?

Most companies will want to do business with the EU. If you can demonstrate you're doing Privacy by Design, that will show good faith to the Europeans.

Anne Cavoukian, Ph.D.
Executive Director
Privacy and Big Data Institute
Ryerson University

Dr. Anne Cavoukian: The GDPR is one overarching privacy and data protection law that will apply to all the 28-member countries of the EU that presently have their own privacy acts. This law is huge in its impact in that it will take over and replace those separate privacy acts. The language of Privacy by Design—data protection by design and privacy as the default—appear in the statute. This is a completely new aspect that has never appeared before in a privacy data protection law.

I urge you, if your company hasn't started looking at this and how it may shift your activities, this is the time to do it. Most companies will want to do business with the EU. If you can demonstrate you're doing Privacy by Design, then clearly that will show good faith to the Europeans.

Data minimization and de-identification are critical from a privacy perspective. You can dramatically reduce re-identification by using strong de-identification protocols combined with the risk of re-identification, as well as using data aggregation and encryption techniques. It is not sufficient to simply strip the personal direct identifiers such as name, social, and home address. You have to strip both direct and indirect identifiers to dramatically minimize the risk of re-identification.

In such instances in which de-identified data was in fact re-identified, you will see that the data was very poorly de-identified at the front-end. It is a myth to think that you can achieve zero-risk anywhere in any aspect. However, you could reduce the risk of re-identification to less than 0.03%, a number comparable to being hit by lightning. You can innovate with de-identified data. It freezes the data for a variety of purposes, such as big data and data analytics.

I don't want you to think of privacy as a negative but as a positive. If you follow the manner of Privacy by Design and advertise it to your customers, then your customers will reward you. The best way to treat personal data ethically is to protect it. Do this up front, embed privacy as the default setting, and lead with that.

KEY RECOMMENDATIONS

BEGIN THE PROCESS OF COMPLYING WITH THE GDPR NOW

The GDPR goes into enforcement May 25, 2018, but you should begin the process of compliance as soon as possible. Even if your business is outside of the EU, the GDPR will affect you if your customers are within the EU. Fines for noncompliance can reach millions of dollars and will have a significant impact on your revenue. The four stages of complying with the GDPR are preparation, production, governance, and reporting.

USE TECHNOLOGY TO MAKE COMPLIANCE MORE EFFICIENT

Use data intelligence tools to do an audit of the data you've collected in the past. Put processes in place that will address compliance in the future. Create a means to respond to user requests regarding their data. Apply a robust content management and reporting system to properly collect, store, and destroy data. Educate your organization so that they understand the requirements for compliance.

USE PRIVACY BY DESIGN TO MEET THE DEMANDS OF YOUR CUSTOMERS

Studies and surveys indicate that concern over privacy is at an all-time high. When you comply with the GDPR and broadcast Privacy by Design as your model, your customers will reward you with repeat business, loyalty, and trust.

ABOUT

ASG Technologies brings peace of mind to every enterprise with information access, management and control within legacy and leading-edge environments. Many Fortune 500 companies trust ASG to optimize their IT investments. With our Enterprise Data Intelligence solution, we give companies deep insights into critical business data. Achieve regulatory governance and compliance requirements with zero gap data lineage analysis, which has allowed customers to see more than 200% savings on time and effort. Our solution provides quick, reliable data intelligence to drive your business forward.

Learn more at www.ASG.com

WBR DIGITAL's team of content specialists, marketers, and advisors believe in the power of demand generation with a creative twist. With senior executives from medium-sized businesses and Fortune 1,000 companies attending more than 100 WBR events each year, we are uniquely positioned to energize your organization's marketing campaigns with a full array of marketing and bespoke content services.