GDPR

A DAY OF RECKONING OR TRANSFORMATION?

EXPERT INSIGHT ON YOUR GDPR JOURNEY:
CHALLENGES, SOLUTIONS AND FIRST-HAND ADVICE

Cyber Resilience ThinkTank

mimecast®

CONTENTS

The GDPR Journey: What You Need to Know

Data. It's fluid, dynamic and alive within your organization. Data knows no limits when it comes to where it flows: the departments, devices, networks, environments and email systems – even third-party vendors – through which it passes seem boundless.

Everyone interacts with data, and the expectation that it should be accessible and available all the time has already been established. But what about control over this data? Specifically, an individual's personal data. What would happen if individuals gained total control over their personal data – things like email conversations, social security numbers, phone numbers, home addresses, HR files and more – the data that lives in virtually countless places in your environment.

What if individuals had the power to request that their entire personal, data-related life be deleted for good?

AN ORGANIZATION LIKE YOURS: MAY 25, 2018

This is the day your relationship with data and privacy could change forever. This is the day when the European Union General Data Protection Regulation (GDPR) takes effect. This is the day when individuals do, in fact, gain control over their personal data and how it's used. This is the day when EU residents can request organizations with personal data about them to stop using it, transfer it, or ultimately, delete it.

So, what is "personal data," anyway?

When it comes to personal data and GDPR requests, context matters. Gartner defines* personal data as any information relating to an identified or identifiable natural personal (i.e., "data subject"). Personal data can be anything from location data, cookies, and employee records and numbers.

Are you prepared to locate any individual's personal data, whether it's living data, archived, being used in a test environment, or in other known-and unknown-places? For the majority of global organizations, the answer is, "Probably not."

A recent Gartner report, GDPR Clarity: 19 Frequently Asked Questions Answered (29 August 2017)

The GDPR Journey: What You Need to Know

EMAIL: A HOTBED OF PERSONAL DATA.

By design, email systems hold a huge amount of personal data, which includes email addresses, phone numbers and other information commonly managed for marketing, customer support and more. GDPR requires that organizations consistently manage backed-up and archived copies, since they are repositories of personal data. In other words, you must be able to efficiently search, find, extract and potentially delete data in your email system, on request.

THE GLOBAL EFFECT.

"My organization isn't based in Europe – I'm off the hook (phew!)."

Wrong.

GDPR impacts organizations globally. If you're a company or government agency that markets, tracks or handles the personal data of EU residents, GDPR obligations apply to you.

Quick Fact: According to Gartner, on May 25, 2018, less than 50 percent of organizations impacted will fully comply with GDPR.

The GDPR Journey: What You Need to Know

This means you may be required to obtain explicit (opt-in) consent from the owners of this data at the time of its collection.

Adhering to GDPR-mandated processes and capabilities will likely require a massive time commitment and investment. Given the global scope of GDPR and its transformative impact, it's imperative that organizations review – and most likely overhaul – the way they handle personal data today. This means having the appropriate technology, processes and staff in place to secure the data and manage live and archived copies meticulously.

If you're not ready to meet these mandatory GDPR requirements, be prepared to potentially pay a massive penalty. And the backlash doesn't stop at fines. You will likely suffer reputational damage, loss of market share, and decreased investor confidence.

GDPR PENALTIES: AN OPERATIONAL KILLER.

If you think putting a process and plan in place for GDPR is overwhelming, you're right. However, brushing-off the May deadline can cost you. Penalties for non-compliance could cost upwards of €20 million or four percent of an offending organization's yearly worldwide revenue, whichever is higher.

THE REPERCUSSIONS ARE REAL. ACCORDING TO THE ANNUAL FINANCIAL REPORTS OF THE FTSE 100:

- **Some companies could see their entire annual profit wiped out if they were to face a four percent fine under GDPR.**
- **Of the 100 companies listed in the FTSE 100, 34 would see their profit wiped out with a four percent fine.**

WHAT'S YOUR TRUST STRATEGY?

A "Trust Strategy" is made up of three things: SECURITY, PRIVACY AND TRANSPARENCY. And data is at the core of this trifecta. Without a firm grasp of the data you collect, store and use, it will be nearly impossible to instill confidence in the products and services your organization provides.

1 CREATE A DATA GOVERNANCE PROGRAM.

This should include a data classification scheme that identifies the data your organization collects and processes, and ranks these categories based on risk to your organization. Create a repeatable process that identifies what data you collect, from whom, where it flows, and its final disposition – whether it's stored, deleted or transferred to a third-party.

2 AUDIT YOUR SECURITY PROGRAM.

It's important to assess your security program and ensure it's protecting the most important data assets you have identified in your data governance program. Test your incident response process! With GDPR requiring as little as 72 hours to notify your local regulators and partners, testing in the middle of an incident will not be ideal.

3 BE TRANSPARENT WHEN YOU COLLECT AN INDIVIDUAL'S DATA.

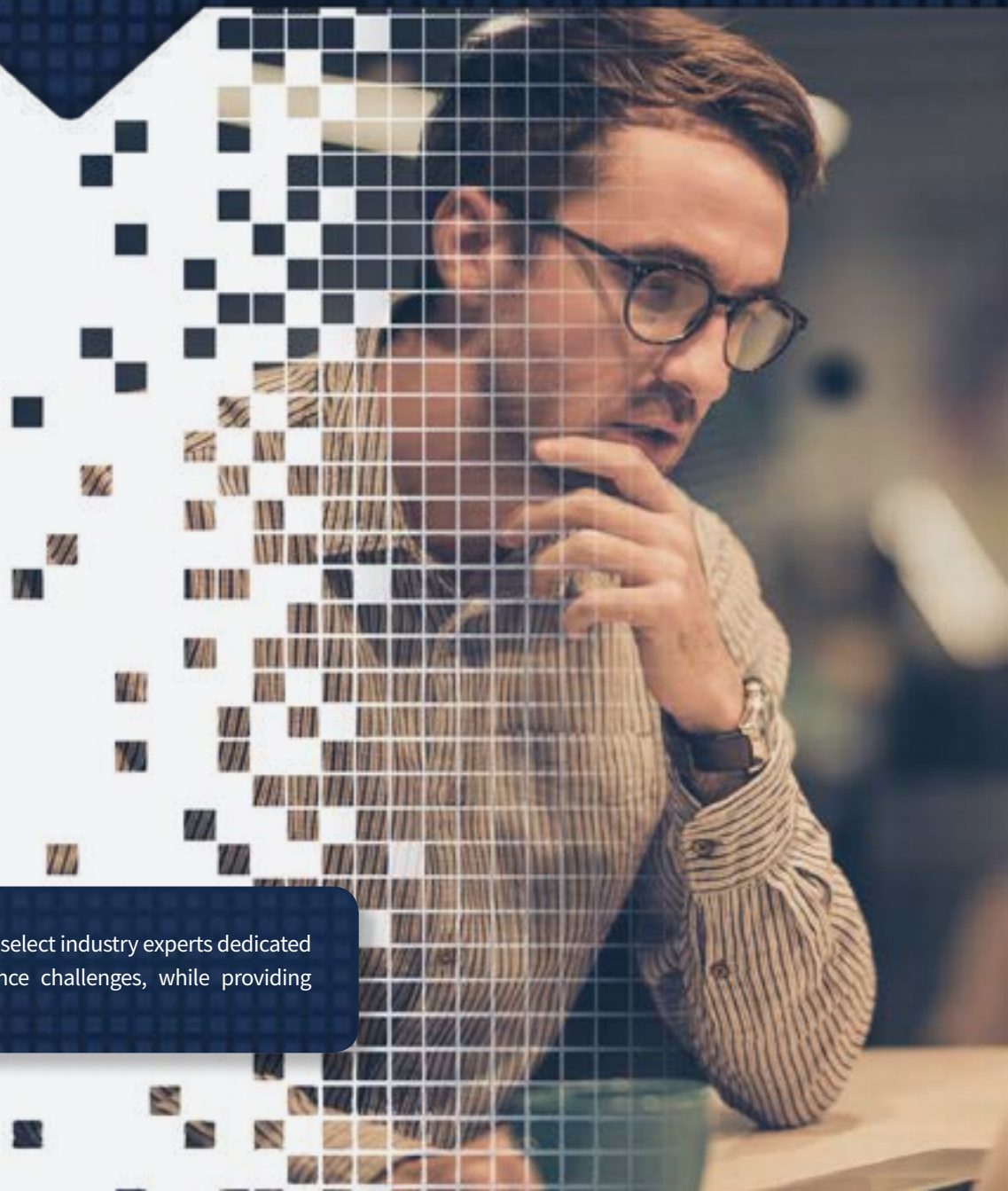
Update your internal and external privacy policies to ensure they accurately reflect how you protect data. And, have a process in place to help guide customers and employees when they have questions or concerns, or want to update their data. This could be as easy as setting up a monitored email inbox and a manual workflow to ensures requirements are met.

GDPR Readiness: An Industry Outlook

As data privacy and data security become paramount issues facing organizations across the globe, you have little choice but to implement, maintain and teach good data practices, especially as external regulations continue to take affect across the globe.

These regulations are far-reaching, and have the power to impact both large-and small-economies, as well as organizations of all sizes and across all industries. But is anyone truly prepared to take on such a massive transformation? And will organizations be able to survive in the wake of these mounting regulations?

Mimecast wanted to get to the root of some of the biggest concerns, challenges and potential solutions when it comes to dealing with GDPR readiness. The Cyber Resilience Think Tank gathered for a roundtable discussion where several industry influencers and experts dove into hot-button topics surrounding GDPR, data security and data privacy.



Cyber Resilience ThinkTank

The Cyber Resilience Think Tank is a group of select industry experts dedicated to bringing to light common cyber resilience challenges, while providing guidance on possible solutions.

GDPR Readiness: An Industry Outlook

READY-OR-NOT: IT'S UP TO YOU.

While there are contributing factors that will impact an organization's GDPR readiness – like the maturity of a company's approach to data management, and whether an organization is in a highly-regulated environment – making data protection and data privacy a priority is your responsibility.

Helen Rabe, Head of Cyber Defense, EMEA at CBRE said, "If data has been treated by an organization as nothing more than a means-to-an-end, it's likely the duty of care toward that data will not have been diligent enough to meet the GDPR compliance requirements. Factor in the volume of data and the types of data used, and this can be a large program of work to remediate."

Rabe continued, "GDPR isn't going away. If you want to stay an active part of the digital ecosystem, and ensure your reputation and revenue generation is in-line with these demands, you will need to respect the notion that data regulation is key to success."

"GDPR isn't going away. If you want to stay an active part of the digital ecosystem, and ensure your reputation and revenue generation is in-line with these demands, you will need to respect the notion that data regulation is key to success."

Helen Rabe
CISO, CBRE

GDPR Readiness: An Industry Outlook

"I CAN MEET THE 72-HOUR RESPONSE TIME," SAID NO ONE.

Under GDPR regulations, organizations have a steep 72-hour window in which to respond to requests. Marc French, Chief Trust Officer at Mimecast said, "Almost everyone I talk to say they are 100 percent not going to make the May deadline. They are so far behind, and getting privacy talent is difficult."

Ari Schwartz, Managing Director of Cybersecurity Services at Venable said, "Zero percent of organizations will be ready to meet the mandatory 72-hour response time. It's very complicated for companies to get a handle on this, especially if they don't have a privacy team in place."

APPLICATIONS ARE MASSIVE DATA GATEWAYS.

Chris Wysopal, CTO and Co-founder at Veracode said, "If data has to be encrypted, made pseudonymous or masked, that means you have to change all your applications – no one is ready to do that. It takes a long time to understand who is going to be accessing what applications and data, and deciding on a strategy for complying around that data."

GDPR Readiness: An Industry Outlook

"Even if you have one application accessing the data in one location, and you decide to encrypt that data, until you have all the applications that access that data being able to decrypt it, you have to have a copy of it in the clear. When is this going to happen for the last legacy system?"

According to Wysopal, it will take companies several years to get to the point where all their data is encrypted. "They still have to run their business; they still have to keep their applications to run their business. To me, this is the long haul – making sure every application still has access to the data it needs to run, and that the data is secure."

Something else to consider when it comes to application security and data: a lot of technologies take snapshots of data all the time for redundancy. "When you delete a file, you have something sitting in the clear in your storage network," said Wysopal. "I don't think people have any understanding of all the places where their data flows in their business."

Evan Blair, Co-founder of ZeroFox said, "Think about when the engagement of the business ends up in the cloud, or in the social media landscape. There is a whole other perimeter outside of your control where data is being shared. Where is this data being transferred from, where is it being shared, and who has access to it?"

> *"When you delete a file, you have something sitting in the clear in your storage network, I don't think people have any understanding of all the places where their data flows in their business."*

CHRIS WYSOPAL
CTO AND CO-FOUNDER
VERACODE

GDPR Readiness: An Industry Outlook

DATA GOVERNANCE IS FOUNDATIONAL.

The core of privacy and security is understanding the data. GDPR readiness is a data governance problem, and something too many organizations tend to skip.

"You need to think about: Where is my data, is it classified, and do I know how to protect it?" said French. "A lot of times, we miss the data governance and data architecture step. Without this, it will be hard to apply security control effectively. If you don't have the data governance foundation, you're going to miss a lot of stuff in the process."

According to Schwartz, "Just encrypting everything only solves part of the problem. How do you know if you've removed a customer's record from everywhere within your organization, unless you know where everything is? You need that data governance foundation."

Blair continued, "In this self-provisioning cloud world we live in, something like Slack can be turned on inside your organization by any employee and shared with an entire system. Customer data has now made its way to things like Slack and HipChat, and IT has it in their test environment – you just can't track it all."

"Data governance is incredibly important. But, all of these new ways for employees to collaborate and share creates a dynamic that I'm not sure anyone will ever be prepared for," said Blair.

> *"Customer data has now made its way to things like Slack and HipChat, and IT has it in their test environment – you just can't track it all."*

EVAN BLAIR
CO-FOUNDER, VP WORLDWIDE CHANNEL SALES, ZEROFOX

GDPR Readiness: An Industry Outlook

FINES, FREAK-OUTS AND BULLS-EYES.

Once the May deadline comes and goes, certain organizations will become the target for maximum fines and penalties for non-compliance – and there will likely be a short acclimation period, especially for U.S.-based companies.

"Organizations are really going to start to freak-out the first time a company gets hit with a $20 million fine," said Schwartz. "The Federal Trade Commission brings a lot of cases; the European debt protection agencies do not. They will start to bring a lot more cases, but it's going to take them time to ramp-up as an enforcement agency."

> *"Organizations are really going to start to freak-out the first time a company gets hit with a $20 million fine."*

ARI SCHWARTZ
MANAGING DIRECTOR OF
CYBERSECURITY SERVICES
VENABLE, LLC

GDPR Readiness: An Industry Outlook

French continued, "U.S. companies will be a target; they will be made an example of. It probably won't be May 2018 but it will likely be August – I bet someone will be made an example of by the end of the summer."

According to French, the U.S. companies that will be under a microscope will be prepared to fight against non-compliance fines. "These are the best-resourced organizations, and they have made tremendous investments to ensure they are not made an example of," he said. "Where we are going to fall down a little bit is downstream – the companies that can't apply the same resources. They are probably going to get hit the hardest."

RISK MITIGATION GOES A LONG WAY.

When it comes to preparing your organization for GDPR, there are many stages of readiness, compliance and protection to consider. You might be wondering where to start, and you're not alone.

"As you go through your GDPR journey, you should hit the areas where you think it's going to be most impactful for you – that's where you start," said French. "If you're an industry where breaches are an issue, you should figure out how to do your 72-hour response as one of the first things you work out. Do a little bit of risk management in your business, and figure out where you're likely to get hit."

Schwartz said, "I agree that the 72-hour breach notification is going to be a new standard. I don't think anyone is ready for this, but it's what companies need to target."

> *"U.S. companies will be a target; they will be made an example of."*

MARC FRENCH
CHIEF TRUST OFFICER
MIMECAST

EXPERT ADVICE: PRIORITIZING GDPR HURDLES

1 TRANSPARENCY AND RESPONSE

What will attract the most attention to you is when you have a breach. The way in which you respond—smoothly and with transparency —when you have an incident will be important. Do this well and it will buy you time and good-will.

2 DATA CLASSIFICATION

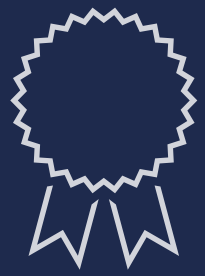
Companies accumulate large amounts of data all over the place without thinking about what's considered to be "personal data" – which is expansive. Understand what GDPR considers to be "personal data" (remember, context matters), and find out all the places where this data resides. Unless something has business value, get rid of it.

3 DATA PORTABILITY

Subject Access Request enables any data subject to request what personal information a company holds on them. This means you must be able to deliver requested personal data in a readable, portable format.

4 RISK MANAGEMENT

Don't try to tackle all your data at once. First, focus on the five or six areas you need to overcome by the deadline. For example: if you have a website, focus on that first; email holds vast amounts of personal data and can be a big risk if not prioritized; if you're tracking through social media, this should be an area of priority. If you don't do a risk management exercise, it will be hard to make progress.



BUILDING A GDPR DREAM TEAM

Finding dedicated privacy talent is difficult, but it's not impossible to assemble a team within your organization to oversee GDPR preparation and risk management. Here's how:

1. Assign **DEDICATED PROGRAM MANAGEMENT** to manage the process.
2. Assemble a **CROSS-FUNCTIONAL OPERATING COMMITTEE** of six people or less to make strategic decisions, and provide governance and oversight.
3. **SPREAD DATA CLASSIFICATION WORK** to the departments that know it best.
4. Have a **GOVERNANCE BOARD MADE UP OF PRIVACY PROFESSIONALS** ready to lean-in and help with the individual functional areas, like data inventory and privacy impact assessment.
5. Keep third-party vendors **COMMITTED TO THEIR CONTRACTS**, and be sure to understand their data flows.
6. **ASSIGN SOMEONE TO BE ACCOUNTABLE**, whether you decide to appoint a Data Protection Officer, there needs to be someone within your organization that is accountable for GDPR.

The Bottom Line

Sure, becoming GDPR-ready is going to be a major challenge for affected organizations. But it doesn't have to be impossible or detrimental to your operations. As you embark on your journey, it's important to revisit – or develop – your cyber resilience strategy. This will help ensure you have the capacity to adapt and respond to adverse cyber events in ways that maintain the confidentiality, integrity and availability of whatever data and services are important to your organization. And, remember: establishing trust and transparency, and implementing the right technology and resources will go a long way.

Here are four easy steps that will help you get started:

1. **KNOW WHAT DATA IS BEING COLLECTED** and stored within your organization.
2. **UNDERSTAND WHERE YOUR DATA GOES** – both internally and externally.
3. **KNOW THE VALUE OF THE DATA YOU COLLECT**, and apply the right amount of resilience protection.
4. **TEST ALL FACETS OF YOUR CYBER RESILIENCE PLAN** for data privacy regularly.

Cyber Resilience ThinkTank

INDUSTRY THOUGHT LEADERS

EBOOK CONTRIBUTORS

ARI SCHWARTZ
MANAGING DIRECTOR OF
CYBERSECURITY SERVICES, VENABLE, LLC

HELEN RABE
CISO, CBRE

MARC FRENCH
CHIEF TRUST OFFICER
MIMECAST

CHRIS WYSOPAL
CTO & CO-FOUNDER
VERACODE

EVAN BLAIR
VP, WORLDWIDE CHANNEL SALES,
ZEROFOX

ED JENNINGS
COO
MIMECAST

JOHN SAPP JR.
DIRECTOR, IT SECURITY & CONTROLS,
CISO, ORTHOFIX , INC.

GARY HAYSLIP
VICE PRESIDENT & CHIEF INFORMATION
SECURITY OFFICER, WEBROOT INC.

MATT CROUSE
DIRECTOR OF INFORMATION SECURITY
TACO BELL

NEIL MURRAY
CTO & CO-FOUNDER
MIMECAST

CATHY HAMMOND
CHIEF SECURITY ARCHITECT
TELEFLEX

JOEL LOWE
HEAD OF INFORMATION SECURITY
SONIC AUTOMOTIVE

ALLAN CAREY
VICE PRESIDENT, BUSINESS
DEVELOPMENT, COFENSE

JIM HANSEN
COO
COFENSE

MALCOM HARKINS
CHIEF SECURITY & TRUST OFFICER
CYLANCE

PHIL OWEN
GLOBAL HEAD OF INFORMATION
SECURITY, IHS MARKIT

STEWART CAWTHRAY
SENIOR DIRECTOR,
PRODUCT SECURITY,
THOMSON REUTERS

JOE GAJDOSIK
DIRECTOR OF IT SECURITY
CURTISS-WRIGHT CORPORATION

MAURICE STEBILA
CISO, IT SECURITY, COMPLIANCE
& PRIVACY OFFICE
HARMAN INTERNATIONAL INDUSTRIES

JASON GUNNOE
CISO
BRIDGESTONE TIRES

Want to learn more about cyber resilience?

Download this E-book now.

Mimecast Limited (NASDAQ:MIME) makes business email and data safer for tens of thousands of customers with millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully-integrated subscription service.