

Insights on  
governance, risk  
and compliance

# When is privacy not something to keep quiet about?

New EU privacy rules are on the way







# EU regulators seek to mandate accountability

In the race to compete in today's digital world, organizations are using social, mobile, big data and analytics, and the Internet of Things (IoT) to gather as much information on their customers as possible, while simultaneously trying to do everything possible to protect their organizations from cyber attacks that come from the outside and within. In this environment, privacy protection can become an afterthought, bolted on to information security programs in an ad hoc manner. Or worse case, organizations haven't thought about privacy protection at all.

For years, regulators and privacy commissions around the world have attempted to legislate privacy protection and develop privacy standards, such as Privacy by Design (PbD) for organizations to adhere and adopt. However, even as regulators pushed accountability, many organizations saw it as more voluntary than mandatory. They were content to address the letter of the law outlined in the legislation as opposed to its spirit – to meet minimal compliance obligations without taking responsibility for their role in protecting their customers' or employees' information.

With the introduction of the European Union's General Data Protection Regulation (GDPR), and the implications for organizations across the globe, the days of organizations leaving the responsibility for privacy protection to someone else is about to end. The EU's GDPR puts the onus of privacy protection where it should be – in the hands of the entities collecting, storing, analyzing and managing personally identifiable information.



54%

of respondents in EY's Global Information Security Survey (GISS) 2015<sup>1</sup> say that their organization has no formalized requirements for using big data while addressing its privacy obligations.



37%

have no formalized requirements to address privacy concerns related to social media.



61%

say that they either have no mandate to minimize or de-identify personal information, or they only do it in unique circumstances.

<sup>1</sup> EY's Global Information Security Survey (GISS) 2015, [www.ey.com/giss](http://www.ey.com/giss)







# Highlights of the GDPR

A little more than 20 years ago, the European Commission introduced the Data Protection Directive 95/46/EC (the Directive). The Directive defined the meaning of personal data and outlined parameters for collecting and managing personally identifiable information.

Technology advancements have fundamentally altered how organizations collect, use and manage data. In light of this, in 2012 the European Commission (EC) embarked on a process to both update, simplify and bolster privacy regulations, and allow EU residents to resume control over their personal data. The culmination of these efforts is the GDPR.

**Released in 2016, and due to come into effect 25 May 2018, the GDPR is an omnibus data protection law that builds upon and expands the Directive. It will ultimately replace the Directive to become the single regulation for data privacy protection.**

The GDPR applies to any organization, regardless of geographic location, that controls or processes the data of an EU resident – and it has teeth. It dictates what data can be collected, the need for explicit consent to gather such data, requirements to disclose any breaches of data, and stronger powers to substantially fine organizations that fail to protect the data for which they are responsible.

## What the GDPR will mean for businesses

- 1 EU residents will gain more control of their personal data.
- 2 Everyone has to follow the same rules.
- 3 Organizations will report to one supervising authority.
- 4 More organizations will need a data protection officer.
- 5 Rules advocate a risk-based approach.
- 6 PbD becomes an enshrined requirement.
- 7 Organizations have 72 hours to report a breach.
- 8 Fines for violations are substantially higher.
- 9 Security is tied to risk.
- 10 The definition of “consent” has been significantly restricted.
- 11 Cross-border transfers are allowed, under certain conditions.
- 12 The restrictions on “profiling” is more narrow than proposed.

The following pages highlight the key issues that we think will affect businesses around the world.

### **EU residents will gain more control of their personal data.**

The GDPR considerably strengthens individual rights over their personal data; this means that organizations will have to provide EU residents with clear and unambiguous information on how their data is being processed and they will have to obtain explicit consent from residents to process it. They will have to allow EU residents to transfer their personal data among service providers, and they will have to allow residents the right to be forgotten by deleting content that they no longer want shared.

1

### **Everyone has to follow the same rules.**

Organizations controlling or processing the data of EU residents, regardless of where they are established within or outside the EU, will have to follow the same rules. In other words, any organization that markets or provides products or services to EU residents will be subject to the GDPR. For all intents and purposes, this makes the GDPR a global law.

2

### **Organizations will report to one supervising authority.**

Under the Directive, organizations must report to a data protection authority in each of the 28 EU member states.

Under the GDPR, these authorities have been consolidated under one supervising authority through which organizations will liaise; this will significantly streamline reporting obligations for organizations and reduce the cost of reporting. The exception to this operational improvement is in addressing complaints: since individuals will be allowed to file a complaint with their local DPA, organizations will have to address those complaints with the DPA the complaint was made to.

3



#### More organizations will need a data protection officer.

Organizations that conduct large-scale processing, or processing of certain types of data as part of their fundamental business activities will be required to appoint a data protection officer. This data may include but is not limited to: an individual's race or ethnicity, religion or philosophy, sexual orientation, health, political opinions, or any other data that may specifically identify and individual (genetic or biometric data).

The data protection officer will be the single source of contact for the supervising authority and will be required to advise upon, and maintain compliance with the GDPR.

4

#### Rules advocate a risk-based approach.

Rather than requiring a one-size-fits-all solution, the GDPR advocates a risk-based approach that allows organizations to tailor their privacy protection programs based on the risks that are most material to the organization. This will include conducting privacy impact assessments (PIAs) for every identified risk and their associated systems and processes.

A risk-based approach elevates privacy protection from a tactical compliance initiative to a strategic imperative.

5

#### PbD becomes an enshrined requirement.

Although PbD has been championed for years by privacy commissions around the world as a leading privacy standard, in our GISS 2015, only 18% of survey respondents indicate that they use PbD as part of how they create new processes and technologies.

Under the GDPR, organizations will now be required to design policies, procedures and systems that follow PbD principles at the outset of every product or process development.

Enshrining PbD as a requirement will force organizations to embed privacy protection into every aspect of their business rather than bolting it on as an afterthought.

6



### Organizations have 72 hours to report a breach.

Rather than having to comply with the breach notifications requirements of each EU member state, organizations will now report data breaches to one supervising authority under a single streamlined breach notification requirement. This requirement stipulates that organizations have 72 hours from the time they discover the breach to notify the authority.

The notification must include the nature of the breach, who had been affected, the potential implications of the breach, and the steps the organization has taken to address it.

7

### Fines for violations are substantially higher.

This is the “teeth” of the GDPR.

Organizations that violate the basic processing principles of the GDPR may be subject to fines totaling as much as 4% of the organization's total global annual revenue.

8

### Security is tied to risk.

Organizations will be required to implement security measures that balance the newest technology with the cost of implementation and reflect the severity and likelihood of risks to an individual's rights and freedoms. This is similar to the Directive; however, the GDPR goes a step further and suggests specific security actions that would be considered appropriate to the risk, such as: pseudonymization and encryption of personal data; the ability to maintain confidentiality, integrity and resilience of systems and services processing personal data; the ability to restore availability and access to data in a timely manner in the event of an incident; and a process for regularly testing, assessing and evaluating the effectiveness of the measures.

Organizations that adhere to either an approved code of conduct or an approved certification mechanism may use these tools to demonstrate compliance with the GDPR's security standards.





**The definition of “consent” has been significantly restricted.**

Where the Directive allows controllers to rely on implicit and “opt-out” consent in some circumstances, under the GDPR, consent must be “freely given, specific, informed and unambiguous.” Specifically, the GDPR requires the data subject to signal agreement by “a statement or a clear affirmative action.” It also places new restrictions on the ability of children to consent to data processing without parental authorization.

10

**Cross-border transfers are allowed, under certain conditions.**

The GDPR allows data transfers to countries that provide an “adequate” level of personal data protection as determined by the EC.

Transfers may also be allowed to non-EU states without an adequate level of personal protection, provided they use other methods of data protection, such as the use of standard contractual clauses or binding corporate rules (BCRs).

11

**The restrictions on “profiling” is more narrow than proposed.**

Under Article 4 (3aa), data processing may be characterized as “profiling” when it (a) involves the automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. This definition implicitly excludes data processing that is not automated.

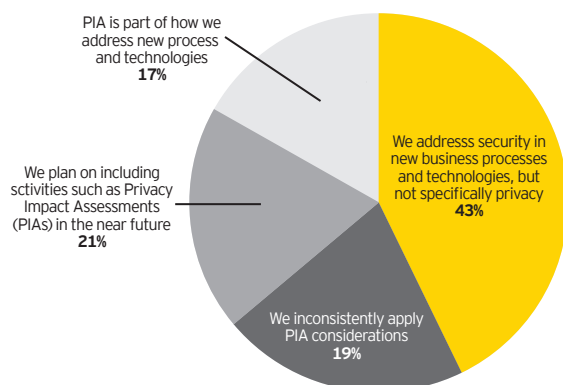
12

### Privacy Impact Assessments will no longer be optional

Privacy Impact Assessments (PIAs) analyze how organizations collect, use, share and maintain personally identifiable information. They help organizations identify and manage privacy risks both within individual projects and throughout the enterprise as a whole. PIAs have been around for quite some time. However, where they were once optional, they are now mandatory. In 2012, the EC's Data Protection Regulation made PIAs mandatory for both public and private sector organizations in Europe – the GDPR extends this requirement.

In a recent joint EY and International Association of Privacy Professionals (IAPP) survey, 59% of privacy professionals indicate that they use PIAs, with approximately 50% saying that they are part of their organizations system development life cycle process. However, in our Global Information Security Survey (GISS) 2015, only 17% indicate that PIAs form part of how they create new processes and technologies, 19% say that they inconsistently apply PIA considerations; and 21% suggest that they have plans to include PIAs in the near future.

The discrepancies among IAPP-EY and GISS 2015 survey respondents may in part be attributed to the respondents themselves: IAPP-EY survey respondents were primarily privacy professionals, whereas GISS survey respondents were predominantly senior information security and technology executives. However, regional differences may also play a role. In the IAPP-EY survey, EU respondents more commonly use internal audit and PIAs; on the other hand, US respondents tend to prefer vendor management platforms, and governance, risk and compliance (GRC) tools.



### Binding Corporate Rules assume greater importance

Binding Corporate Rules (BCR) are a set of internal guidelines that define global policies for organizations to transfer personal data within the same corporate group of entities, but across geographic jurisdictions. They offer a robust data protection compliance package that enables consistency of data protection within the organization.

Given that the GDPR will require organizations to implement comprehensive policies and procedures to meet – and demonstrate – compliance obligations associated with the GDPR, there is no better time to either have BCR certification, or to pursue it.

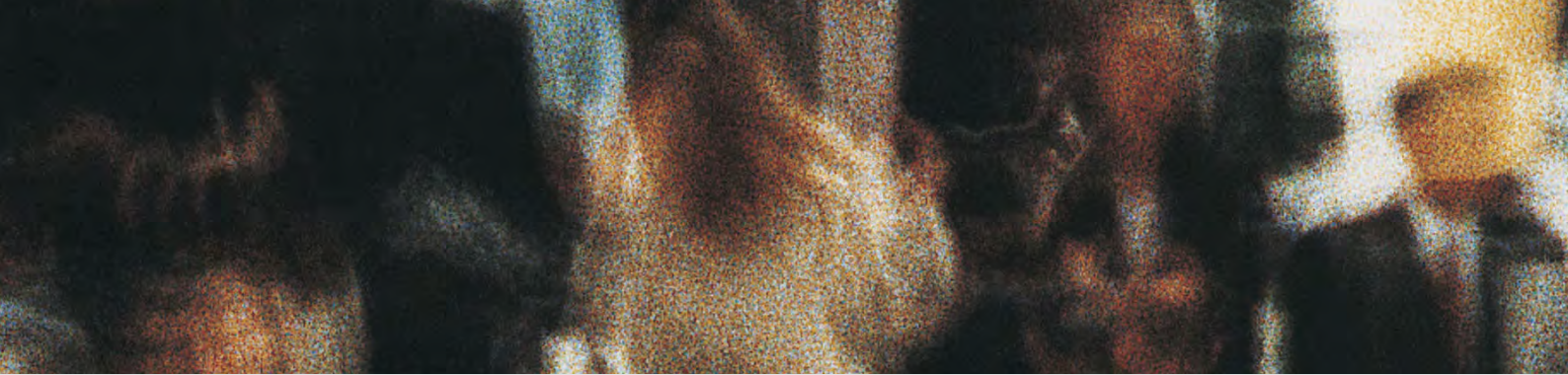
#### Achieving BCR status can benefit organizations in three ways:

1. BCR certifications are designed by and tailored to each individual organization's business model, operations, processes and culture.
2. Meeting the rigor associated with BCR will mean that a organization will be more likely to comply with data protection laws globally.
3. The GDPR expressly promotes BCR, which means that an organization that has BCR may be more likely to be viewed more favorably by the EU's supervising authority that oversees the implementation, monitoring and compliance of GDPR.

To date, approximately 80 organizations have successfully applied for BCR status. However, when we asked respondents as part of the GISS 2015, of the 43% of respondents who plan on transferring personal information out of the EU, only 10% are in the process of or have already obtained BCR approval.

With the level of effort, time and cost associated with pursuing BCR certification, organizations that need to adhere to GDPR would do well to start the planning process for obtaining BCR status sooner rather than later.





## Big changes ahead for processors

**Although all organizations doing business in the EU will be impacted by the GDPR, processors will have more adjustments to make than others.**

Processors are individuals or organizations that process personal data on behalf of the data controllers. Until now, processors have been required to keep personal data confidential and secure as instructed by the controller. Further, the controller has remained responsible for compliance with data protection principles, liability and any associated fines for non-compliance.

Under the GDPR, processors will become subject to the same compliance obligations, legal requirements, and punishment for noncompliance as controllers. The GDPR does not explicitly provide an explanation for the shift, other than its clear position that individuals need to have legally enforceable rights. Controllers will still carry the lion's share of the burden when it comes to compliance and liability, but processors will no longer be off the hook.

Specifically, processors will have to adjust to the following changes:

► **Direct application of the data protection law**

The GDPR will apply to EU-based processors processing personal data whether the processing takes place in the EU or not. It will also apply to processors located outside of the EU if it offers goods and services to EU residents or processes their personal data in any way (behavior monitoring).

► **Demonstrated accountability**

Processors with more than 250 employees will have to create and maintain records of all of their data processing activities, even if their services do not actually interact with customer data (such as cloud providers). Processors will also have to employ a data protection officer if the processor processes sensitive data or regularly monitors individuals on a large scale.

► **Direct responsibility for data security**

Processors and controllers will now both be responsible for data security, which may include encryption and pseudonymization, as well as a requirement to maintain systems and services with integrity, confidentiality and availability.

► **Dual responsibility for compliance**

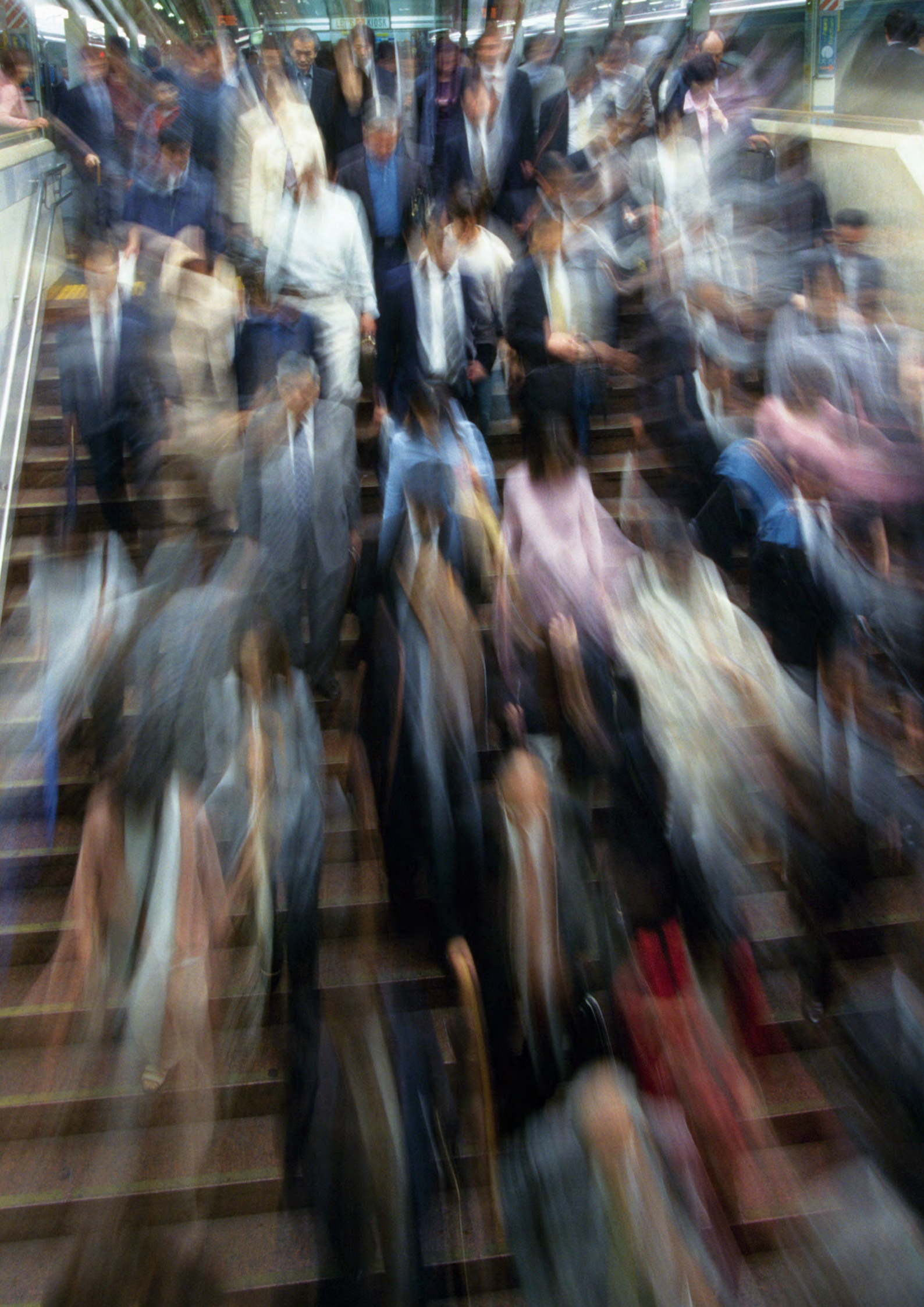
Processors will now be equally responsible for compliance with data transfer rules, and will have to prove they have adequate systems in place, such as Binding Corporate Rules (BCR) when transferring data to countries without adequate protections.

► **Approval for subprocessors**

Processors will now have to seek approval from controllers before engaging subprocessors, and must extend to the subprocessor the same contractual provisions agreed to with the controller.

Ultimately, these changes mean that processors will have to collaborate more closely with controllers to maintain the privacy and confidentiality of personally identifiable data. They will be equally responsible for security and compliance, and must be able to demonstrate accountability for their processing activities.







# It's time to take ownership for information practices

The days of laissez faire, or ad hoc privacy policy-making are about to come to the end for organizations.

With the GDPR, organizations will now have to take ownership of their information practices, be accountable for all associated privacy risks across the enterprise in the course of doing business, and be able to prove the veracity of their programs. Organizations that don't, risk reputational and financial damage that could be far more than costly – it could be ruinous.

The impact of the GDPR will be felt globally for two important reasons:

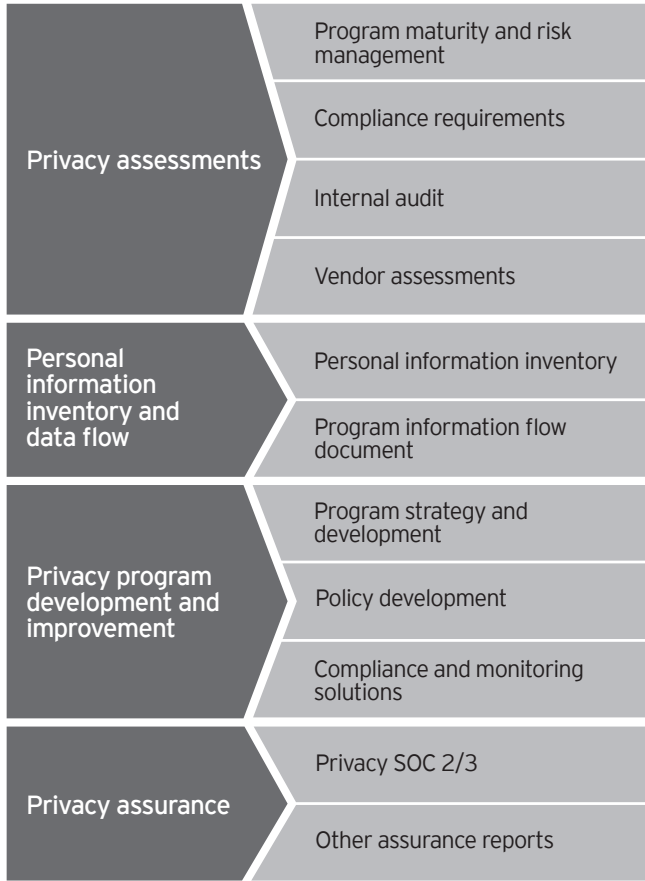
- 1. The regulation applies to EU residents' personal information regardless of the location of processing. For multinational organizations, that is likely to mean any location where global sales or HR activities take place in.
- 2. The greater consistency in applying privacy requirements across such a large number of countries in the EU, coupled with the increased attention on binding corporate rules (BCR), is now more likely to become the de-facto standards for large organizations to build their privacy programs against.

For too long, privacy management was an ongoing exercise of tracking differences between regulations and parsing the comments made by regulators and enforcement bodies. While this compliance oriented mentality will not completely leave the privacy field, we are more likely now to see the attention of privacy professionals to the effectiveness of information management. Regulations and policies are important, but without efficient privacy controls, effective data and organizational governance and the monitoring of their implementation, compliance with such a significant regulation will not be met.

## How can EY help?

EY offers a range of privacy assurance and advisory services. We are ready to help our clients assess their programs against the GDPR requirements, design practical recommendations and help the monitoring of the program's performance. With many successful BCR development projects behind us, we are able to help our clients address the needs of their cross border transfers across the globe.

Our privacy services include, but are not limited to:



# Want to learn more?

*Insights on governance, risk and compliance* is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our Insights on governance, risk and compliance series at [ey.com/GRCinsights](http://ey.com/GRCinsights).



*Can privacy really be protected anymore:  
Privacy trends 2016*  
[ey.com/privacy2016](http://ey.com/privacy2016)



*Creating trust in the digital world:  
EY's Global Information Security  
Survey 2015*  
[ey.com/GISS2015](http://ey.com/GISS2015)



*IAPP-EY Annual Privacy Governance  
Report 2015*  
[ey.com/IAPP-EY](http://ey.com/IAPP-EY)



*How do you find the criminal before  
they commit the cybercrime?: a close  
look at cyber threat intelligence*  
[ey.com/CTI](http://ey.com/CTI)



*Using cyber analytics to help you get  
on top of cybercrime: third-generation  
Security Operations Centers*  
[ey.com/3SOC](http://ey.com/3SOC)



*Enhancing your security operations with  
Active Defense*  
[ey.com/activedefense](http://ey.com/activedefense)



*Cybersecurity and the Internet of Things*  
[ey.com/IoT](http://ey.com/IoT)




*Achieving resilience in the cyber ecosystem*  
[ey.com/cyberecosystem](http://ey.com/cyberecosystem)



*Cyber program management: identifying  
ways to get ahead of cybercrime*  
[ey.com/CPM](http://ey.com/CPM)





## **If you were under cyber attack, would you ever know?**

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of backoffice systems and into critical infrastructures such as power generation and transportation systems.

Anticipating cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then collaborate with you to create innovative answers that help you activate, adapt and anticipate cybercrime. Together, we help you design better outcomes and realize long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.




About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2016 EYGM Limited. All Rights Reserved.

EYG no: 01206-163GBL  
ED None

 In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities – strategy, customer, finance, IT, supply chain, people advisory, program management and risk – with a complete understanding of a client's most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory's high-performance teams also draw on the breadth of EY's Assurance, Tax and Transaction Advisory service professionals, as well as the organization's industry centers of excellence, to help clients realize sustainable results.

True to EY's 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital perspectives into every service offering.

EY Advisory's global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to create innovative answers that help their businesses work better.

The better the question. The better the answer. The better the world works.

Our Risk Advisory Leaders are:

EY Global Risk Leader		
Paul van Kessel	+31 88 40 71271	<a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a>
EY Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	<a href="mailto:amy.brachio@ey.com">amy.brachio@ey.com</a>
EMEIA		
Jonathan Blackmore	+971 4 312 9921	<a href="mailto:jonathan.blackmore@ae.ey.com">jonathan.blackmore@ae.ey.com</a>
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	<a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a>
Japan		
Yoshihiro Azuma	+81 3 3503 1100	<a href="mailto:azuma-yshhr@shinnihon.or.jp">azuma-yshhr@shinnihon.or.jp</a>

Our Cybersecurity Leaders are:

EY Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	<a href="mailto:kallan@uk.ey.com">kallan@uk.ey.com</a>
EY Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	<a href="mailto:bob.sydow@ey.com">bob.sydow@ey.com</a>
EMEIA		
Scott Gelber	+44 207 951 6930	<a href="mailto:sgelber@uk.ey.com">sgelber@uk.ey.com</a>
Asia-Pacific		
Paul O'Rourke	+65 8691 8635	<a href="mailto:paul.o'rourke@sg.ey.com">paul.o'rourke@sg.ey.com</a>
Japan		
Shinichiro Nagao	+81 3 3503 1100	<a href="mailto:nagao-shnchr@shinnihon.or.jp">nagao-shnchr@shinnihon.or.jp</a>
Global Privacy Leader		
Sagi Leizerov	+1 703 747 0899	<a href="mailto:sagi.leizerov@ey.com">sagi.leizerov@ey.com</a>