www.pwc.com

Contents →

EU Data Protection Reforms

Challenges for Business

July 2014

Contents

Introduction

The European data protection regime is governed by the European Data Protection Directive 95/46/EC. The directive was introduced in 1995—before the widespread use of complex consumer technology. In response to calls for an overhaul and update of European data protection legislation, a proposed General Data Protection Regulation is currently proceeding through the European legislature.

The draft regulation seeks to harmonize data protection law across European member states, is significantly more prescriptive than the directive, and would introduce widespread data protection changes as well as greatly increased financial sanctions for noncompliance. Such changes are likely to raise significant challenges in regard to data protection compliance for all businesses (regardless of the location of their establishments) that operate or provide goods and services within the European Union (EU).

Main challenges involve:

a. service providers or producers (defined as entities that develop systems for the processing of personal data—for example, hardware or apps) that are not subject to the directive today but that will have to adapt quickly in order to comply with the new law
b. appointing a Data Protection Officer (DPO) with sufficient expertise
c. meeting amended breach notification requirements
d. staying up-to-date on developments related to consent and legitimate interests as grounds for data processing and balancing them with the individual's right to be forgotten
e. embedding privacy into operations
f. avoiding increased financial penalties and reputational damage

To ensure compliance with the draft regulation once it comes into force (which will most likely be in 2016), companies must implement adequate policies, procedures, and processes to comply with the changes the regulation introduces. The details of the changes—and the challenges they present for organizations—represent a significant departure from the current system and require additional action to achieve compliance: With the reform, organizations based outside the EU will have to apply the same rules. Measures must be implemented to deal with and enhance policies and processes involving (1) monitoring, (2) breach notification, (3) incident detection and response, (4) enforcement of privacy through systems' life cycles, and (5) formation of a governance group or appointment of a DPO.

Additional measures must be introduced to cover adequate training for staff and restriction of access to data when possible.

The principles governing the processing of personal data in the draft regulation do not differ significantly from those in the directive. Therefore, implementing measures now to become compliant with the directive would put an organization in an advantageous position for complying with the regulation in a cost-effective way once the regulation comes into force.

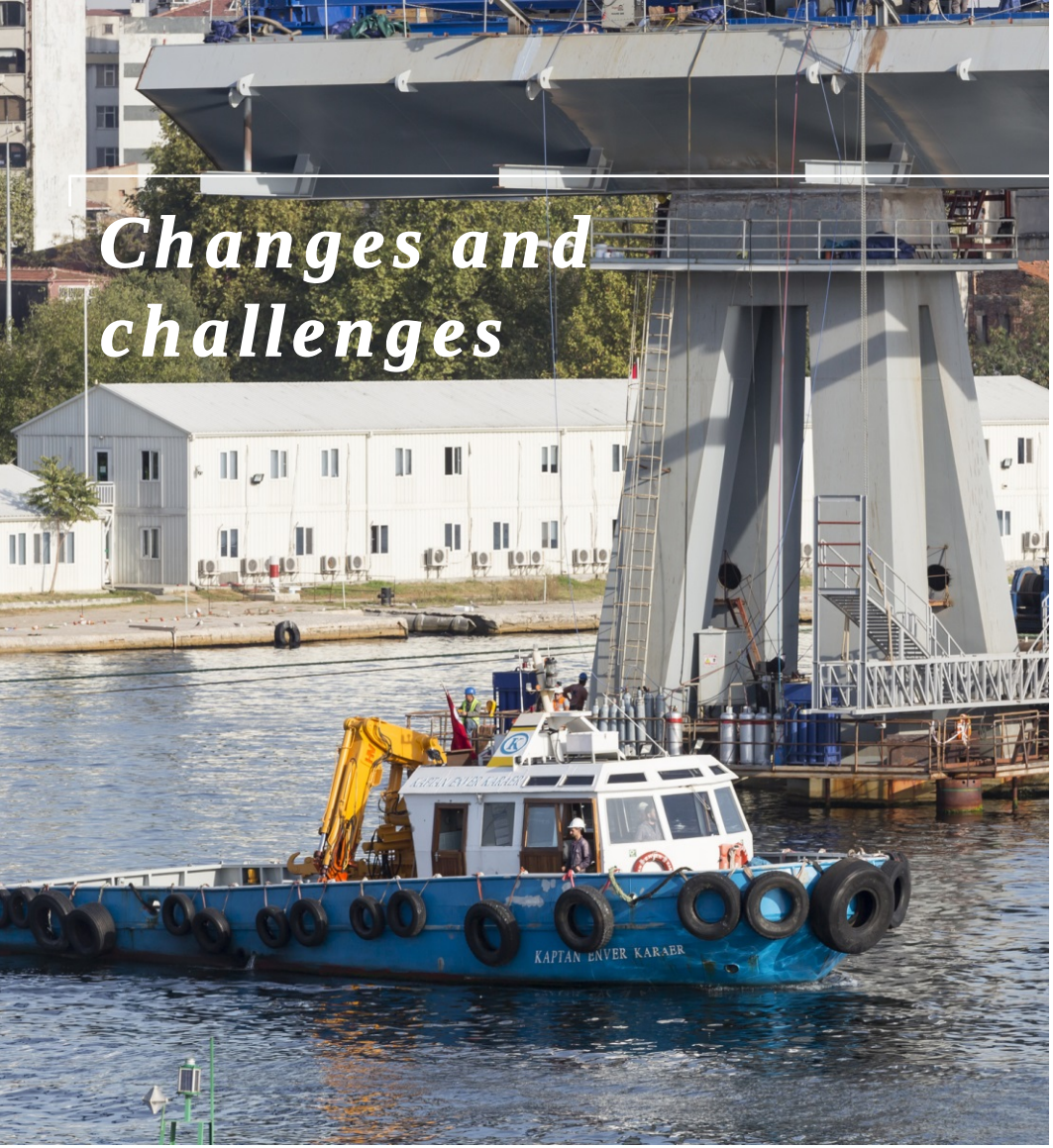
In conclusion, the draft regulation offers businesses certain benefits, including consistency and the potential to achieve cost reduction in the area of data protection compliance. However, for businesses to avoid severe penalties and potential reputational damage, the regulation does require businesses to take compliance seriously and combat the challenges mentioned.

The need for change

The EU's current data protection framework was established in 1995 by the European Data Protection Directive 95/46/EC to harmonize data protection laws across the EU. The directive required each member state to introduce implementing legislation that would give its provisions effect, such as the Data Protection Act 1998 in the UK. Member states were also required to appoint a supervisory authority (e.g. the Information Commissioner's Office in the UK, CNIL in France, and GIODO in Poland). An important aim of the directive was to harmonize data protection laws across Europe, but methods of the implementation of laws and the approaches by data protection authorities differ among member states. In particular, such issues as notification requirements and attitudes to enforcement are treated differently by different member states. The result is that multinationals with presences in member states across Europe are left to negotiate patchworks of differing requirements, which typically require significant resources in terms of time and expertise.

Drafting the directive began in the late 1980s—before widespread use of the Internet, Web version 2.0, tablet computers, smartphones, and social-networking sites. The Data Protection Directive raised awareness of the importance of personal data, but as technology became more and more advanced and as practices changed, the need for an overhaul of the law became more apparent. Reform of EU-wide data protection legislation is not an insignificant task (the Data Protection Directive took five years to negotiate), and progress is protracted at the European level.

In response to widespread calls for an overhaul of the directive, in January 2012 the European Commission published the draft regulation. Since that publication, the draft regulation has been the subject of considerable scrutiny and extensive debate. In December 2012, the European parliamentary Committee on Civil Liberties, Justice and Home Affairs (LIBE) published a report advocating 3,000 amendments to the draft. The majority of the changes proposed by the report were approved by the European Parliament on March 12, 2014. For the draft regulation to become law, the next step is for the Council of the EU and European Parliament to agree on the final text. It is hoped that the final text will be agreed on in the European Council Summit during October 23–24, 2014. The text of the current draft regulation provides that the regulation would take effect after two years, in 2016. Unlike the directive, the regulation would take direct effect in member states rather than operate through implementing legislation. The draft regulation is indeed more rigorous, but that's because it seeks to avoid the currently existing patchwork of legislation.



Changes and challenges

The data protection principles that apply to the processing of personal data are largely the same in the draft regulation as in the directive. However, the draft regulation is three times longer and significantly more prescriptive than the directive it would replace, and it would introduce widespread changes (explained later). The changes are likely to pose significant new data protection compliance challenges for businesses operating in the EU, as well as for businesses established outside the EU but whose products and services are directed at Europeans.

Scope and application of the draft regulation

The directive draws a distinction between *data controllers* and *data processors*. **Data controllers** are the individuals, companies, or bodies that decide the manner in which and the purposes for which personal data gets processed. **Data processors** do not make decisions regarding personal data but instead process *on behalf of* data controllers; for example, an outsourced payroll provider, server host, or software-as-a-service provider is likely to be a data processor. The directive applies only to data controllers and not to data processors. Data controllers are required to contractually bind data processors to certain obligations when they appoint them, but in the event of a breach, the data controller still bears liability under the directive.

The draft regulation will apply to data controllers and data processors established in the EU, as well as to those established outside the EU if their goods or services are directed at EU residents or if they monitor Europeans. It also introduces a new category of producers: those that develop systems for the processing of personal data—for example, hardware or apps.

The extended scope of the regulation apportions risk between organizations and their service providers. However, service providers that to date may not have had to concern themselves with data protection issues are likely to have to get up to speed quickly.

Appointing data protection officers (Articles 35 and 36)

Under the directive, companies must generally register with the data protection authority in every jurisdiction where they have entities established—a process called notification. Notification consists of filing a description of the company's processing activities with the authority and keeping the files up-to-date. However, each data protection authority's requirements differ from those of other authorities, so notification can be a resource-consuming exercise for large multinationals with presences in numerous member states. The draft regulation abolishes the requirement to notify with data protection authorities and instead introduces a requirement to appoint a DPO. The draft regulation currently lists four categories of organization as follows that must appoint DPOs.

i. Public authorities or bodies
ii. Organizations carrying out the processing of more than 5,000 data subjects
iii. Certain processing activities such as regular and systematic monitoring or profiling of data subjects
iv. Organizations whose core activities consist of processing special categories of data

An organization must ensure that its DPO has expert knowledge of data protection law and practices; and that level of knowledge must be proportional to the level of risk of the processing. The DPO's other duties must not cause a conflict of interest with the position. For example, placing the DPO within the legal function may create conflict as the role of a legal advisor is different to the responsibilities of the DPO as contemplated by the regulation. The DPO should be appointed for a term of four years and can be dismissed only because of no longer fulfilling the conditions required for the performance of the job's duties, which means the DPO cannot be dismissed for convenience. The DPO must be independent and must report to the data controller or data processor's management—likely to be interpreted as the board of directors.

Organizations are required to communicate the name and contact details of the DPO to the relevant data protection authorities and to the public. However, if an organization decides not to appoint a DPO, it must communicate the reasons for its decision to the appropriate supervisory body. In practice, organizations fulfilling one of the four aforementioned criteria must appoint a DPO unless there is a very good reason not to.

For organizations required to appoint a DPO under the regulation, one of the challenges will be to find the right expertise. And that leads to a further challenge for companies established outside the EU, companies providing goods and services for EU residents, and companies with limited privacy and data protection expertise. Because there may be too few appropriately qualified privacy professionals to fill the requirements mandated by the draft regulation, one possible solution could be to outsource the function to an outsourced data protection officer service.

Breach notification (Articles 31 and 32)

The directive does not require data controllers to inform the relevant data protection authority of a data breach. However, the draft regulation would introduce a requirement to inform the relevant data protection authority of a personal data breach within 72 hours of the data controller's becoming aware of it. The draft regulation defines a personal data breach as (1) accidental or unlawful destruction, loss, or alteration or (2) unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

The data protection authority must be informed of the details of the nature of the breach (including numbers of data subjects and data records concerned), must be given the contact details for the DPO, must be sent recommended measures to mitigate adverse effects, and must be offered descriptions of the consequences of the breach and of the measures taken to address it. The draft regulation also introduces a requirement that the data protection authority keep a public register of the types of breaches communicated.

When a personal data breach is likely to adversely affect the data subject's privacy—such as in cases of identity theft, fraud, physical harm, significant humiliation, or damage to reputation—the data controller must then communicate the data breach also to the data subject. However, notification to data subjects may not be necessary if the supervisory authority is satisfied that the data was protected by appropriate encryption. US-based companies have been dealing with breach requirements for several years, but the proposed regulation requires notification of data breaches under shorter time constraints and for broader types of data than required under security-breach-notification laws enacted under US state laws. Plus, the EU regulation handles encryption differently: Under the proposed regulation, notification to the supervisory authority is required even if the data is encrypted. This is different from the US model, wherein notification to either the individual or the regulatory body is not required if the data is encrypted. The financial implications resulting from the duty to inform individuals of a data breach potentially include loss of reputation, loss of business, and, in the worst cases, a drop in share price. Such reputational risks could outweigh the heavy penalties the draft regulation would introduce (explained later).

One-stop shop: Lead authority (Articles 54 and 73)

As explained earlier, the directive requires data controllers established in more than one member state to register with the data protection authority in each jurisdiction in which they are established, unless an exemption applies. This presents a significant challenge for large multinationals. To meet that challenge, the draft regulation would introduce a one-stop-shop system, with a designated lead data protection authority that would act as a single contact point for an entire multinational group. The draft regulation would also grant aggrieved individuals the right to lodge complaints with any member state's supervisory body, which would then coordinate with the relevant authorities to take further action. Clearly, the one-stop-shop would streamline the process for both organizations and individuals. However, complex multinational companies would still be left with deciding their main establishment within the EU.

Grounds for processing: Consent and legitimate interests

Both the directive and the draft regulation provide a number of grounds for the processing of personal data, one of which the data controller must establish as a first step to ensuring that such processing is lawful. The grounds are as follows:

i. the data subject has consented to the processing.

ii. the processing is necessary for the execution of a contract.

iii. the processing is necessary for compliance with a legal obligation of the data controller.

iv. the processing is necessary to protect the data subject's vital interests.

v. the processing is necessary for the performance of a public-interest task or for the exercise of official authority.

vi. the processing is necessary for the purpose of the legitimate interests of the data controller, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

The grounds under the draft regulation are largely the same as those of the directive, but there are significant developments regarding *consent* and legitimate interests.

The draft regulation clarifies the definition of consent—significantly.

Under the draft regulation, a data subject's consent must be given freely and must be a specific, informed, and explicit indication of the data subject's wishes either by a statement or a clear affirmative action by which they signify their agreement to the processing of personal data related to that data subject. In addition, the draft regulation introduces significant changes by:

i. placing the burden of proof on the data controller

ii. giving data subjects the right to withdraw consent at any time for future processing

iii. preventing consent from being construed as a legal basis for processing when there is a significant imbalance between the data controller and the data processor—such as in an employer-employee relationship

iv. stipulating that the execution of a contract or the provision of a service cannot be made conditional on consent to the processing or use of data that is not necessary for executing the contract or providing the service

v. stipulating that consent loses its effectiveness as soon as the processing is no longer necessary for carrying out the purpose for which data were collected

Legitimate interests

It was mentioned previously that consent provides one ground for ensuring processing is legal. An alternative option regularly relied on by European businesses is the data controller's legitimate interest. This ground evolved to address low-risk processing activities when none of the other grounds for processing is appropriate and when obtaining consent involves a disproportionate effort in the circumstances. To meet the legitimate-interests ground for processing, a controller must explicitly and separately inform the data subject of the legitimate interests pursued, document and publish the reasons for believing that its interests override, and remind the data subject of the data subject's right to object.

The draft regulation provides guidance about the appropriate use of the legitimate-interests ground by giving examples of instances that a data controller's legitimate interests would override—namely, in the following circumstances.

i. Freedom of expression, media, and arts

ii. Enforcement of the data controller's legal claims—or preventing or limiting damage by the data subject

iii. Data provided for the execution of a contract

iv. Professional business-to-business relationships

v. Registered, not-for-profits and charities for collecting donations

The draft regulation also gives examples of instances that a data subject's legitimate interests override—namely, in the following circumstances.

i. When there is risk of serious damage to the data subject

ii. In special categories, such as when biometric or location data is processed

iii. Data subject's reasonable expectations that data will be processed only for a specific purpose

iv. When the processing includes profiling

v. When the data is made accessible to a large number of people or large amounts of data about the data subject are processed

vi. When the processing may adversely affect the data subject—in particular, could lead to defamation or discrimination

vii. When the data subject is a child

Data controllers relying on legitimate interests as a ground for processing data will have to revisit their existing processes to ensure the new criteria get met. However, data controllers established in European countries that do not currently recognize the legitimate-interests ground under the existing system may welcome this change to the law.

The right to be forgotten

The right to be forgotten, which Article 17 of the draft regulation would introduce, has been subject of much discussion. The data subject's right to be forgotten and right to erasure appears in Article 17 of the draft regulation. Those rights aim to address data protection risks online. If data subjects no longer want their data processed or stored and there is no legitimate reason for keeping it, the data must be removed from the system, and data controllers must instruct any third parties with which they have shared the data to do the same.

The right to be forgotten and the right to erasure are not absolute rights; there are legitimate reasons for a data controller to retain data, which may include newspaper archives, freedom of expression, or freedom of the media. Companies will have to carefully consider how they manage that obligation and will have to have appropriate policies, procedures, and processes in place.

The right to data portability

The proposed regulation also provides the right to data portability, which will make it easier for a data subject to transfer personal data between service providers. This further creates a challenge for global providers: to make sure that the data they collect or process is in a consistent format that will facilitate the exercise of the right to data portability.

Privacy by design and default (Articles 23 and 33)

Data controllers must implement systems so that they process personal data in accordance with the draft regulation. By default, systems should process only minimum data for the minimum duration necessary for the purpose of processing. And producers and processors must ensure their products and services enable controllers to meet the draft regulation's requirements. In other words, systems that process personal data will have to have privacy baked in. Controllers must also conduct privacy impact assessments in relation to processing activities that present privacy risks, such as when processing involves systematic and extensive evaluation of personal aspects relating to a natural person. This requirement will significantly change current practices wherein the privacy impact of a new system is usually considered only as an after-thought, if at all. However, for complex global organizations (both controllers and processors), a challenge would be to identify and evaluate existing business processes that need to be retrofitted in order to account for privacy-by-design principles.

Transfer of personal data to third countries (Articles 40–45)

The draft regulation maintains so-called adequacy decisions, which allow personal data to be transferred out of the EU. Such a decision is an acknowledgment that a given non-EU country ensures an adequate level of data protection through its domestic law or international commitments. Approved binding corporate rules may also cover data processors that process the personal data of EU residents on behalf of data controllers.

To allow data transfers from the EU to the USA, the US Department of Commerce and the European Commission developed the Safe Harbor framework, approved by the EU in 2000. Safe Harbor's future is currently under discussion. The Commission identified 13 recommendations to strengthen the framework in the areas of transparency, redress, enforcement, and access by US authorities. The US Department of Commerce is looking to make amendments to the framework that would meet or even surpass recommendations made by the European Commission but also keep the regulatory compliance cost at a minimum. It is expected that Safe Harbor will become strengthened by the summer of 2014. However, it remains to be seen exactly which changes will be implemented or whether Safe Harbor will be suspended if the Commission deems changes inadequate. This creates a significant challenge for US-based companies currently operating under the Safe Harbor framework, because they may have to revamp their processes and procedures to incorporate changes to the current framework or participate in other transfer mechanisms (binding corporate rules, standard contractual clauses, or explicit consent) in the event Safe Harbor gets suspended.

Penalties (Article 79)

Supervisory bodies are empowered to impose administrative sanctions that must be effective, proportionate, and dissuasive in each case. They may issue written warnings (for first-time and unintentional breaches), conduct regular data protection audits, and—under the current version of the draft regulation—introduce sanctions against enterprises (regardless of their establishment in the EU or outside the EU and providing goods and services for EU residents) in the form of fines of up to 5% of worldwide annual turnover or €100 million, whichever is greater.

To determine the type, level, and amount of administrative sanction, the supervisory authority must take into account all relevant factors, including the nature and seriousness of the infringement, whether it was intentional or not, and the degree of harm data subjects suffered. The rationale behind the proposed heavy fines is to elevate data protection to a board-level concern with a view to embedding privacy into business cores. It follows that we are likely to see large fines in practice as examples to other organizations.

Recommendations

It remains to be seen what the final text of the draft regulation will include once the European Parliament and the European Council have finished debating the text's form. In its current rendering, the draft regulation introduces many changes that present new changes and challenges for businesses. To address those changes and challenges—and to avoid financial and reputational penalties—companies must implement changes to their policies, processes, and procedures before the regulation comes into force. Companies—specifically, multinationals with complex business models and global presences—should consider taking the following steps.

i. Conduct a data protection review to understand current and planned EU footprint and exposure

ii. Evaluate existing compliance programs and structures

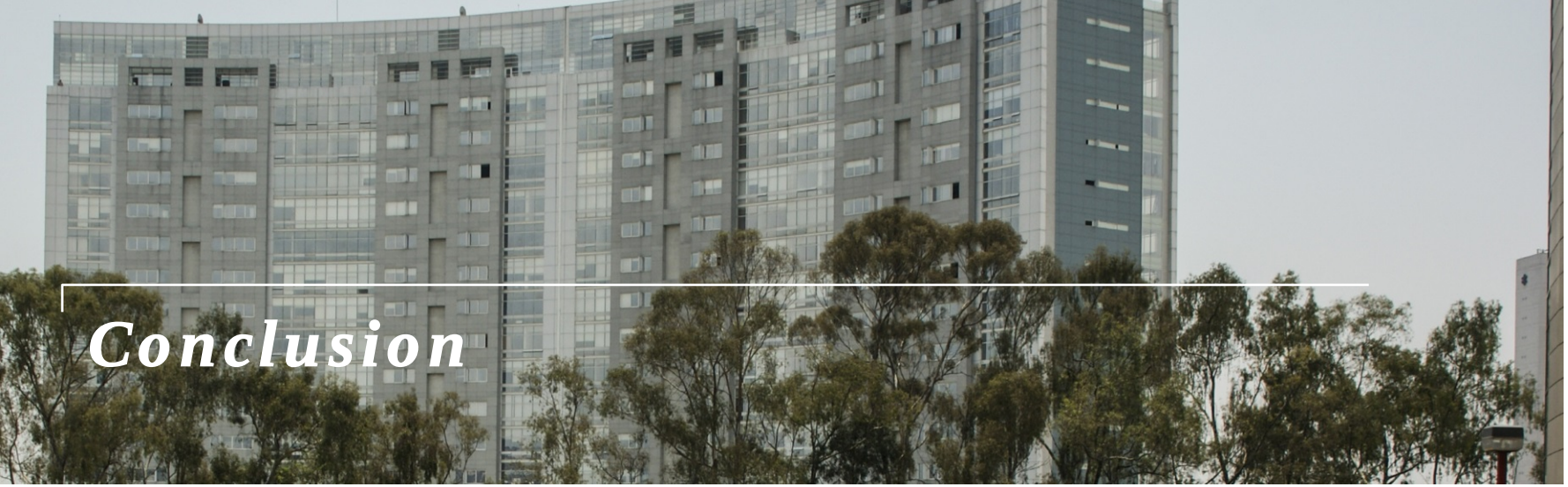
iii. Identify EU personal data collected and stored

iv. Analyze existing data processing activities and cross-border and third-party data flows, and determine potential gaps and weaknesses

Companies must take adequate measures to rectify identified gaps, including training of staff and developing and implementing ongoing compliance monitoring programs that would alert management to potential violations in time to implement amendments before sanctions are imposed.

Given that the data protection principles governing personal data under the regulation remain largely the same as in the directive, the introduction of measures now to ensure organizations are compliant with the requirements of the current directive is a good step toward helping businesses become able to comply with the draft regulation in a cost-effective way and toward protecting themselves once the regulation becomes effective.

The draft regulation offers a means for businesses to save significant costs in the area of data protection, but those businesses must ensure they are fully compliant in order to avoid substantial financial penalties and damage to reputation. Many organizations worry about the potential financial penalties and may be motivated primarily by the risk of sanctions. However, some organizations are already using data protection compliance as a positive differentiator to attract customers. Public awareness of the importance of privacy is beginning to result in customers' voting with their feet and seeking the goods and services of providers that respect their rights.



Conclusion

The draft regulation harmonizes data protection across the EU and may benefit businesses in a variety of ways. It offers consistency and certainty for businesses in terms of their data protection activities and liabilities across the EU and enables businesses to have more-integrated EU-wide data protection policies and management. Businesses should save time and money with the removal of the requirements to register and update notifications with multiple data protection authorities, which are replaced by introducing a DPO and a lead authority for the group's main establishment.

Additionally, on one hand, the regulation is more fit for purpose in the electronic age—including but not limited to cloud and mobile technologies and social networking. On the other hand, the draft regulation raises new challenges, including reliance on data subjects' consent and on the monitoring of data subjects' amends to their consents. It becomes harder to rely on legitimate interests for processing, and increased frequency of data protection and privacy audits adds a barrier to compliance and increases the risks of extreme financial penalties and reputational damage.

An immediate challenge for businesses will be the resourcing of the DPO requirement, because there do not appear to be enough qualified DPOs in the current market.

To combat those challenges, companies must take action to implement adequate policies, processes, and procedures to comply with the changes the regulation introduces and to avoid heavy sanctions when it comes into force. Organizations with strong procedures for protecting personal data will have a competitive advantage on a global scale at a time when the issue is becoming increasingly compelling.

To have a deeper conversation about how this subject may affect your business, please contact:

Carolyn Holcomb
Partner
Data Protection and Privacy Leader
Risk Assurance
(678) 419-1696
carolyn.c.holcomb@us.pwc.com

Jay Cline
Principal
Data Protection and Privacy
Risk Assurance
(612) 596-6403
jay.cline@us.pwc.com

Joe DiVito
Principal
Data Protection and Privacy
Risk Assurance
(412) 355-8067
joseph.v.divito@us.pwc.com