

The GDPR Demands 75k DPOs

iapp



**Where Will They
Come From?**

Introduction

As President and CEO of the International Association of Privacy Professionals, I have been thrilled to see the privacy profession blossom in the 15 short years since our organization was founded. From just a handful of people around the world, struggling to understand how new technology and old law should fit together, we have grown to 26,000 strong – and counting.

Yet even that is not nearly enough for the job ahead.

While this document lays out the demand for privacy professionals – data protection officers, specifically – created by the EU's General Data Protection Regulation, surely you know that those DPOs are just the tip of the iceberg. As every organization around the world becomes increasingly dependent on data to drive their activities, so too does it become increasingly important that they have trained professionals at the ready to analyze use cases, identify risk, and apply the deep thinking that privacy and data protection often require.

No two countries apply data privacy law in exactly the same way. Every regulatory agency is some varying combination of educator and enforcer, but all of you have a vested interest in seeing privacy understood and respected. Please know that the IAPP stands at the ready to work toward these common goals.

The community, training, education, and tools that we provide are aimed, first and foremost, at helping people do the job of privacy better. We hope that this makes your jobs easier, along the way. If I, or my staff, can provide you with further research or resources to help you with your efforts in any manner, please let me know.



J. Trevor Hughes
President and CEO, IAPP
jthughes@iapp.org

The GDPR Demands 75k DPOs: Where Will They Come From?

No country is immune: The industrial economy is giving way, or has already given way, to the digital economy, where data is currency and there is insatiable demand for it. Recognizing this, governments around the world are passing new legislation to require that sensitive data, personal data, be adequately protected, transparently used, and that the rights of data subjects to maintain control of their data are not violated.

Leading the way is the EU's General Data Protection Regulation, what many are calling the world's most comprehensive privacy law, reaching across 28 Member States and encompassing virtually every way that data might be collected and used. However, we see any number of other national laws coming quickly on the GDPR's heels, many of them modeled after it.

As every regulator is aware, of course, a law is only as good as the populace's ability to comply with it, and the legal mechanisms of enforcement that back it up. With so many new laws coming onto the books, and with the GDPR's vast reach, it is no wonder that we are seeing organizations and enforcement agencies alike racing to staff their data protection offices with qualified professionals.

How, we must ask ourselves, can we produce enough privacy professionals in time to fill all of the positions being created? Such, in part, is the mission of the International Association of Privacy Professionals, which has deeply explored this issue. We offer here an estimate of the scope of the demand and some thoughts on how it may be addressed.

How, we must ask ourselves, can we produce enough privacy professionals in time to fill all of the positions being created?



GDPR Has a Global Reach

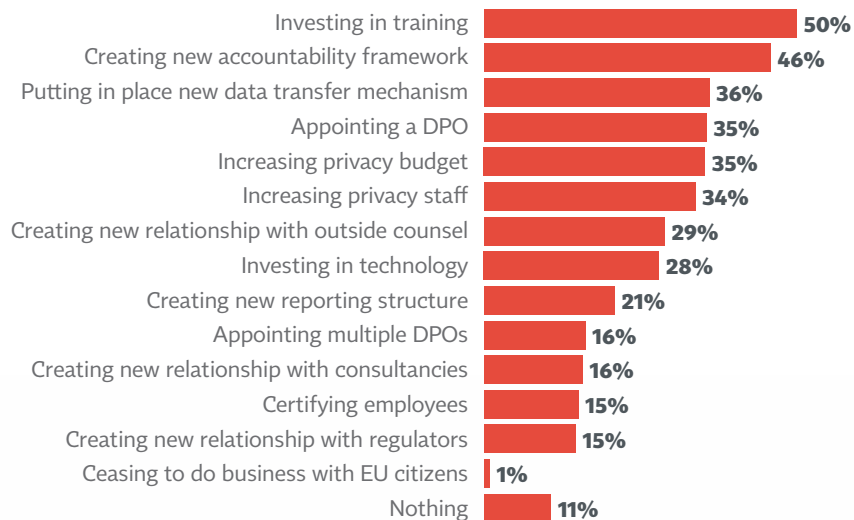
The long-anticipated European Union General Data Protection Regulation takes effect in May 2018. Pursuant to Article 3, the GDPR's many requirements apply “to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union.”

In other words, the EU's jurisdiction over the collection and processing of EU citizen data is global. That means the obligation to comply with it is equally global.

Who will lead this effort within organizations that do business in, and business with, the EU?

Among the GDPR's new obligations on data controllers and processors is the requirement to employ a data protection officer. The DPO position has existed under German law for some time, and some organizations use that title for those tasked with data protection compliance, but for the remainder of the EU Member States — as well as most other countries doing business in the EU — making sense of and responding to this new professional role can be daunting.

Steps Being Taken To Prep for GDPR (Among Those Falling Under GPDR)



Organizations around the world are taking major steps to comply with the GDPR, including investing in training, creating a new accountability framework, and appointing a DPO.

Source: IAPP-EY Privacy Governance Report 2016.

For, indeed, the DPO is a professional position. The GDPR expressly requires DPOs to be “designated on the basis of professional qualities” and to have “expert knowledge of data protection law and practices.” DPOs will work closely with Data Protection Authorities, serving as their contact inside the data controller and helping to ensure GDPR compliance. DPOs will need to understand data protection obligations well enough to train staff on proper data handling practices and must keep up with changes in law, policy, and technology. They must also understand how to build, organize, implement, manage, and constantly update data protection programs.

This is not the job description for a low-level compliance manager. This is clearly a savvy operator within the business or public body, someone who can serve many constituencies, evaluate risk, and prioritize efforts.

Thousands of DPO Positions Will Be Created

Article 37 of the General Data Protection Regulation requires controllers and processors of personal information to designate a data protection officer when:

- (a) The processing is carried out by a public authority or body (except courts); or**
- (b) The controller’s or processor’s “core activities” require “regular and systematic monitoring of data subjects on a large scale” or consist of “processing on a large scale of special categories of data.”**

The IAPP has estimated, conservatively, as many as 75,000 DPOs will be needed to manage EU citizens’ personal data around the world.

As many as 75,000 DPOs will be needed to manage EU citizens' personal data around the world

Using publicly available statistics from Eurostat, we calculated the approximate number of large EU enterprises (defined by the EU as those with more than 250 employees) in each of 13 non-financial industry sectors: mining and quarrying; manufacturing; electricity, gas, steam and air conditioning supply; water supply, sewerage, waste management and remediation; construction; wholesale and retail trade and repair of motor vehicles; transportation and storage; accommodation and food service activities; information and communication; real estate activities; professional, scientific and technical activities; administrative and support service activities; and repair of computers and personal and household goods.

To be conservative, we excluded all micro, small and medium-sized companies, even though many of them will no doubt engage in the large-scale monitoring or processing of sensitive data and thus be required under the GDPR to appoint a DPO. Further, we assumed only one DPO per company, though many large companies will employ multiple DPOs.

We then made a number of calculated assumptions:

- **We assumed that any company with at least 5,000 employees would process and monitor human resource data on a “large scale” and would thus need a DPO for such processing. Going by average employee data supplied by Eurostat, we determined roughly 15 percent of all large enterprises had at least 5,000 employees.**
- **We also assumed that, due to the data-intensive nature of their operations, up to 50 percent of large companies for the following industry categories would need a DPO: transportation and storage (e.g., airlines); accommodation and food service (e.g., hotels); and professional, scientific and technical activities (e.g., accounting firms).**
- **Finally, we assumed 100 percent of the large enterprises in “information and communication” would need a DPO.**

Based upon these assumptions, we estimate that 11,790 non-financial private sector enterprises in the EU would require a DPO under the GDPR.

We further assumed that 100 percent of all financial institutions (7,226) and life insurance enterprises (535) would require a DPO due to the nature of their business.

For public authorities, according to a 2010 report on Public Employment in EU Member States, there were around 19,000,000 public administration employees in the EU. At an average of 1,000 employees per agency — the average size of a “large” private enterprise in the EU — that amounts to 19,000 large public agencies across the EU, which will need a DPO and be too large to be covered by a DPO at a senior agency. We can assume some sharing among them — conservatively one DPO for every five agencies — for a total of approximately 4,000 DPOs required in the public sector.

Lastly, we assumed that many U.S. companies obliged to comply with the GDPR would also require a DPO, and of those companies we assumed that most of those who self-certified under the Safe Harbor (4,500) are likely included in that number. Further, we discovered in the 2016 IAPP-EY Privacy Governance Report that roughly half of those regularly transferring personal data from the EU to the U.S. were Safe Harbor certified, so that implies a total of 9,000 companies in the U.S. would require a DPO.

We then took that number of 9,000 companies required in the U.S. and compared it to the most recent international trade figures published by the European Commission, thus creating a Euros-per-DPO figure that we could then apply to the EU’s top trading partners, those countries with EU adequacy decisions, and other countries with robust privacy laws and establishments.

We estimate that 11,790 non-financial private sector enterprises in the EU would require a DPO under the GDPR.

Our research thus suggests that the number of DPOs required under the GDPR will be, at a minimum, 75,000, worldwide. **See tables for country-by-country breakdown;** for the EU Member States, we applied the EU-wide methodology to each Member State using publicly available total employment data.

EU Member States			
Belgium	466	Lithuania	141
Bulgaria	323	Luxembourg	30
Czech Republic	607	Hungary	418
Denmark	279	Malta	30
Germany	4596	Netherlands	891
Estonia	75	Austria	792
Ireland	185	Poland	1445
Greece	373	Portugal	512
Spain	1914	Romania	677
France	2705	Slovenia	96
Croatia	175	Slovakia	228
Italy	2568	Finland	228
Cyprus	30	Sweden	533
Latvia	96	United Kingdom	3103

Top 10 EU Trading Partners	
US	9000
China	7568
Switzerland	3682
Russia	3068
Turkey	2045
Norway	1790
Japan	1688
South Korea	1330
India	1125
Brazil	972

Other Common Trading Partners	
Canada	920
Morocco	460
Hong Kong	715
Singapore	715
Australia	613
Mexico	767
Israel	460
Argentina	255
New Zealand	237
Uruguay	51

The DPO On-Ramp

The big question now is: Where will these 75,000 data protection officers come from?

Of course, some DPOs will be trained and promoted within the company, and some positions will be outsourced to service providers, like law firms and consultancies, offering DPO services to multiple clients. But many DPOs will be full-time professionals created as new positions and forming part of a new and emerging professional corps.

Assuming that many of these new full-time professionals will have little to no background in privacy and data protection, how should they best acquire “expert knowledge of data protection law and practices”?

According to the European Data Protection Supervisor’s [paper on “Professional Standards for Data Protection Officers,”](#) DPOs require ongoing training after they have been appointed. They also should be encouraged to obtain certifications in data protection and to continue to develop their professional skills and competencies through networking with other data protection professionals and attending conferences and events. The EDPS specifically recommends the IAPP’s CIPP/E certification.

Similarly, Eric Lachaud, in his article [“Should the DPO Be Certified?”](#) for Oxford University’s International Data Privacy Law journal, states: The most appropriate certification for the DPO is a combination of the IAPP’s Certified Information Privacy Professional credential for EU professionals (CIPP/E) and Certified Information Privacy Manager (CIPM).

The CIPP/E, CIPP/US, CIPM, and CIPT (Certified Information Privacy Technician) credentials are certified under ISO standard 17024:2012.

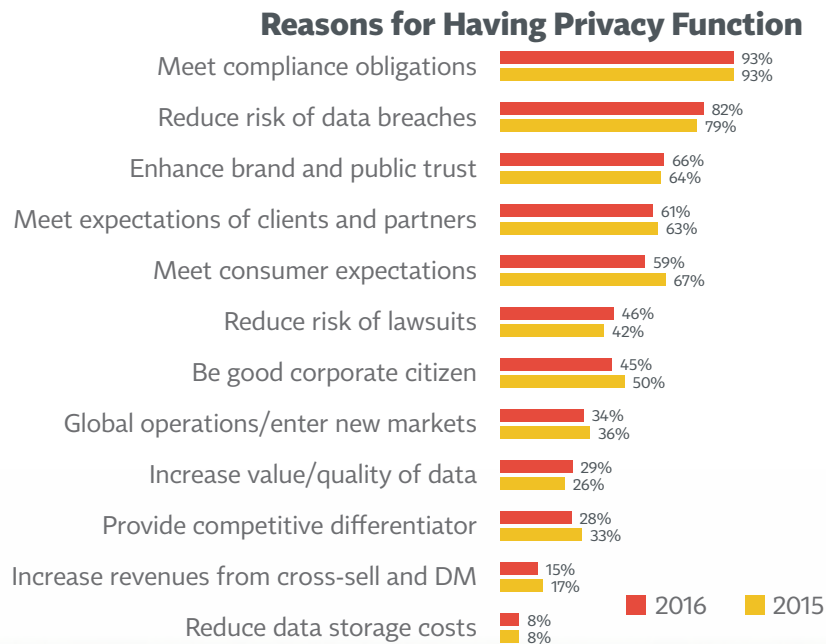


Professionals also need the opportunity to grow and develop their skills, beyond simple learning and certification.

The IAPP has worked diligently to create a center of gravity for the burgeoning data protection and privacy technology industry. As technology companies from around the world develop products to help DPOs with their compliance obligations, the IAPP is there to offer free trials and samples, product reviews, and opportunities for DPOs to be trained on using information technology tools in their data management functions.

A DPO can only fully understand his or her responsibilities through listening to peers, understanding burgeoning best practices, and having access to tips of the trade that veterans are constantly imparting to their new colleagues in the field.

The IAPP offers a host of free networking events in more than 70 countries around the world, in hundreds of cities. New recent “KnowledgeNet” chapters include Istanbul, Bangalore, and Buenos Aires. Those are in addition to the major conferences the IAPP holds each year in Brussels, Washington, Singapore, London, and the west coast of the United States.



Organizations certainly focus on complying with privacy regulation, but also see privacy as key to enhancing brand and meeting customer expectations.
Source: IAPP-EY Privacy Governance Report 2016.

The Future

May of 2018 is rapidly approaching. Organizations around the world are preparing for the GDPR by increasing budgets, hiring staff, employing consultants and external counsel, and creating frameworks for compliance.

By extension, as the DPO is in effect an arm of the Data Protection Authority, organizations' GDPR-preparation efforts are in lockstep with those of regulators. And it's not only EU DPAs who are preparing oversight and enforcement mechanisms, but also their colleagues around the world who are looking to collaborate through efforts like the Global Privacy Enforcement Network and the Asia Pacific Privacy Authorities.

If citizens' data protection and privacy rights are to be adequately protected, then this pool of 75,000 DPOs must be quickly created and well trained. Regardless, the world will have a privacy law that is only as good as organizations' ability to comply with it.



About the iapp

With more than 26,000 members in 86 countries, the International Association of Privacy Professionals (IAPP) is the world's largest and most comprehensive data protection and privacy resource. The IAPP helps to define, support and improve the privacy profession globally, delivering the knowledge necessary to ensure data protection and privacy through membership, events, training, certification and more.

Membership

- Individual membership delivers the tools and resources necessary for heightened job performance, personal career advancement and myriad networking opportunities.
- Corporate membership illustrates an organization's commitment to data protection and information privacy.

News

- Stay current on all things privacy — around the world and around the clock, at iapp.org/news. We make it easy, with daily news updates, expert analysis, original reporting, legislative alerts, and opinion pieces from the influencers making the news.
- You can also have it all sent directly to your inbox with IAPP email newsletters, daily top global stories, weekly regional updates, and more. Choose from the [Daily Dashboard](#), [Privacy Perspectives](#), [The Privacy Advisor](#), the [Europe](#), [Canada](#), [Asia-Pacific](#) or [Latin America](#) digests and others.

Events

- The IAPP hosts the industry's premier events, where data protection and privacy professionals from around the world gather to learn, network and share ideas.

Training and Certification

- The IAPP delivers premier training that equips Data Protection Officers and other data protection professionals with the knowledge and skills required to comply with the GDPR and legislation around the globe.
- IAPP-trained staff gain improved decision-making skills and are better able to reduce the risk of data breaches and prevent privacy incidents.
- Having privacy-trained staff demonstrates an organization's commitment to customers, partners, regulators and employees.
- IAPP certifications help distinguish privacy professionals from others in the field, conveying advanced skills and commitment to data privacy protection.

Learn more about all the IAPP offers, including CIPP/E and CIPM trainings—recommended by Oxford University's International Data Privacy Law Journal for the “expert knowledge of data protection law and practices” DPOs and other privacy professionals will require to be successful under the GDPR.

Please visit iapp.org/traindpos today.