European Union General Data Protection Regulation (GDPR)

Building a Successful Compliance Programme

The GDPR applies to all organisations that process, store or use data about EU citizens. Even if an organisation does not have operations in the EU, if the business employs EU citizens or has customers and/or suppliers who are EU citizens, it must comply. Penalties for noncompliance with the GDPR can be significant, with potential fines of up to 4 percent of a company’s global revenues.

Organisations subject to the new legislation have a two-year grace period from the date the GDPR came into effect until 25 May 2018 to review their current practices and procedures and become compliant. The not insignificant grace period may have some business leaders believing time is on their side, but they should not underestimate the complexities of achieving GDPR compliance.

Many organisations will find they have much work to do, especially if they have operations across multiple countries, as many such organisations struggle to meet fully the existing data protection legislation requirements consistently on a global basis. We believe many such businesses will need to take a different approach to managing data privacy in the future. A few organisations may need to rethink their business model entirely.

In short, organisations must move quickly to determine the level of effort required to comply with the new regulation and to institute appropriate remediation plans where needed. This document outlines key steps that organisations should take to set up a successful GDPR compliance program, and presents several considerations these businesses should keep in focus throughout the process.

### Choosing the Right Programme Leadership

The GDPR is ultimately a compliance requirement. As such, responsibility for project will often most naturally reside with compliance and/or in-house legal teams. However, this does not mean that these functions are necessarily best placed to own the project. In fact, based on our experience:

- **We do not believe that the legal team should take the lead, in most cases.** This can result in organisations focusing too much attention initially on defining policies, procedures and model contracts.

- **The compliance function may also not well-suited to lead the programme.** To achieve GDPR compliance, the business likely will need to apply significant risk judgements and be pragmatic in its interpretation of the legislation. Even though the compliance function is adept at highlighting risks, it is not typically responsible for making risk-based decisions.

- **The information security team should not take the lead, either.** GDPR is not an information security programme. Security is a component of the programme and is often coupled with privacy. However, it is only one of many considerations required for GDPR compliance – and the information security focus is often overstated. Information security teams also tend to place too much emphasis on data protection or data loss prevention. These activities are important but potentially of lower priority than other data privacy processes that companies must adopt to comply with the GDPR.

Fundamentally, a GDPR compliance programme is about changing behaviours, which can be very difficult to execute effectively across a large multinational company or supply chain. Therefore, someone with the capabilities and authority to impact change across the extended organisation on a global basis should lead the initiative. The day-to-day administrative components of this role can be

---

delegated, but ultimate accountability must be high up if an organisation is serious about affecting change.

This is why we believe accountability for the GDPR programme should be assigned to somebody like the chief operating officer (COO) or equivalent in the senior management team. We also believe that this person, or someone at or close to this person’s level, should be the data protection officer (DPO).

**Selecting the right DPO will be the key to GDPR compliance success for many organisations.**

In most cases, the DPO will not be the person currently fulfilling the role under existing legislation. The GDPR creates many new obligations for the DPO. The person in this position must have:

- An understanding of what it takes to run an enterprise wide programme and the authority to make the changes necessary to embed appropriate controls in business processes.
- The ability to apply sound judgement and make risk-based decisions quickly in order to meet reporting deadlines.
- The ability to drive change in the organisation and establish a defensible strategy for deployment.

**Starting the Process**

We believe compliance programmes are much more successful if they take a “top-down” approach. Organisations therefore should review their business operating model and revenue streams first to understand what sensitive private data they are capturing and how they are using it. This exercise will help focus attention on the most challenging, high-risk areas.

The process of identifying these high-risk data elements, if done effectively, will form part of the **Data Protection Impact Assessment (DPIA)**. Article 35 of the GDPR requires organisations to perform this assessment.

Only when the business has decided how to respond to the issues it faces in the high-risk areas, reflecting corporate risk appetite, should it attempt to encapsulate this in policy documents. Referencing actual examples from the DPIA can make policies relevant and actionable. A top-down approach also ensures policies are tailored to high-risk user communities and associated business processes.

Initially, the priority areas of focus will be:

- Highly sensitive personal data that the organisation holds in bulk.
- Data that the organisations holds and uses (and/or potentially sells on) in ways that the data subject (e.g., customer) might not be aware of or has not consented to.

Companies need to quickly determine whether they hold any of these data elements and if so, whether they would be comfortable going public about how they are using private data.

Some organisations will not have any data that meets the criteria above; for these businesses, GDPR compliance should be relatively straightforward.

---

**Failing to Enforce EU Citizens’ Civil Rights and Obtain Consent Could Lead to Penalties**

In many cases, an isolated data loss event results in limited damage – provided that the organisation can demonstrate it executed timely reporting of the data loss and has contained the amount of data lost.

Under the GDPR, penalties could be more severe if an organisation fails to implement processes to enforce EU citizens’ civil rights, such as the right to be forgotten, or to obtain appropriate consent from EU citizens to use their data in a certain way (e.g., data transfer).

For example, a business could face fines if an investigation into suspected data loss finds that the company was misusing an EU citizen’s data (e.g., the name of a citizen who requested to be forgotten remains on a mailing list that a company employee maintains manually). Penalties could be imposed even if no data loss occurred.
Penalties could be more severe for failing to implement processes to enforce citizens’ civil rights, such as the right to be forgotten (allowing citizens to request companies remove their private data), the right to transfer data (allowing citizens to request private data is transferred from one supplier to another) and/or failure to obtain appropriate consent. Significant penalties could therefore be applied even if no data loss event has occurred if an investigation is performed, perhaps as a consequence of data being misused after an EU citizen has requested to be forgotten, due to their name remaining on a mailing list that is being maintained manually by somebody within the organisation.

Other Considerations
We recommend that organisations keep the following considerations in mind when developing their GDPR compliance programme:

- **The GDPR could be disruptive to digital transformation programmes.** GDPR requirements could have a significant impact on an organisation’s planned digital initiatives if that company is reluctant to request consent from EU citizens to use their data to derive value and/or if consumers do not give consent en masse. Organisations that are using data from historical customers unlikely to provide consent, or that do not have a direct relationship with a customer, may face particular difficulties.

  Organisations could find themselves spending significant resources on digital transformation programmes only to find they cannot derive the anticipated value due to restrictions arising from the GDPR. Therefore, when conducting the DPIA, organisations should consider not only current activities, but also future activities that may form a part of digitalisation initiatives.

- **Data processors can no longer hide behind data controllers.** Under legislation put in place in response to the EU Data Protection Initiative, any action against an organisation must be taken against the data controller by the Data Protection Authority commissioner. Depending on contractual arrangements, the data controller may be able to pass this risk on, in part or in full, to the data processor. However, it is not unusual for confidentiality agreements to make it difficult for a data controller to “name and shame” a third party publically.

  Under GDPR, the Data Protection Authority can impose penalties directly on the data processor. This could have significant implications for organisations that process sensitive personal data on behalf of third parties. Thus, organisations will need to focus as much on priority data that they manage on behalf of others as they do on data that they own.

  Another key observation of the new legislation is that the data controller is not in control of data breach reporting; as a result, if a data controller is withholding information, it could be immediately apparent to the Data Protection Authority. Given the tight reporting timelines under the new regulations, organisations will need to make quick decisions. This is one reason we believe the DPO should be a senior person in the organisation.

- **Brexit adds complications.** Far from exempting companies from complying with the GDPR, as many companies have hoped it would, Brexit will actually complicate matters for many organisations that are subject to GDPR. The timetable for the GDPR will run ahead of any formal exit by the United Kingdom from the EU. At minimum, there is likely to be a one-year period, or longer, when the GDPR fully applies.

  However, the United Kingdom Government generally supports the GDPR and its underlying principles and we believe it is likely continue to do so once it leaves the EU under its own legislation. Official guidance to U.K. companies is therefore to “press ahead” with evaluations and plans to prepare for GDPR compliance.
Should the U.K. government decide not to adopt or align to the GDPR in full, there will be significant complications for U.K. companies that trade with the EU, for non-U.K. businesses with a significant EU hub in the United Kingdom, and for companies that work with suppliers that base their EU data-processing centres in the United Kingdom.

In these circumstances, a data transfer between the EU and the United Kingdom would be deemed a data export. There are various options that companies can adopt in these circumstances, including:

- Standard contractual clauses
- Binding corporate rules (all countries, including the United Kingdom, after Brexit)
- U.S.-EU Privacy Shield and other similar bilateral agreements

Organisations also may need to consider relocating data, changing suppliers and/or re-engineering systems. However, we do believe, for the reasons outlined above, that it is unlikely the U.K. government will adopt such a policy.

**Immediate Actions**

All organisations that need to comply with the GDPR should take the following steps immediately:

- **Assign the DPO**: The DPO role must be filled quickly to ensure the GDPR compliance program has the leadership needed to drive success. The business should also provide the assigned DPO ample time to consider the impact of, and to affect, change.

- **Carry out a top-down analysis**: A good starting point for developing a GDPR compliance program is a quick top-down analysis to identify highly sensitive and/or high-risk items. This exercise also will enable the DPO to quickly understand the complexities that GDPR presents to the business, and to engage early with senior executives to define a strategy for compliance.

- **Complete the DPIA**: The organisation must complete a top-down analysis and capture the results in a formal DPIA that meets GDPR requirements (Article 35). This comprehensive analysis will form the basis for formal planning activities.

- **Prioritise actions**: The business must prepare a comprehensive action plan to respond to all potential risk areas identified in the DPIA. Even though it will not be possible to prepare a complete set of actions until the DPIA is complete, the organisation should not delay in commencing remediation of high-risk areas identified in the initial top-down analysis.

- **Plan remediation**: The business should create a detailed project plan, with clearly defined roles and responsibilities, that is supported by an appropriate resourcing schedule. It also should prepare an analysis of critical dependences. Organisations should not underestimate the importance of training, awareness and change management activities related to this plan.

- **Revisit the DPIA**: GDPR compliance is an ongoing requirement – not a onetime project. It is important for the organisation to establish a process to revisit the DPIA on a regular basis and review remediation plans as needed.
About Protiviti

Protiviti is currently working with organisations around the world to help them assess the implications of the GDPR on their business, and establish successful compliance programmes that reflect the risk culture of the organisation. We recognise that there is no one-size-fits-all approach to GDPR compliance and that every organisation is different. We are currently working with organisations to perform top-down analyses of their business models to identify key risk areas. In addition, we are helping executive teams to define GDPR compliance strategies that seek to minimise the impact on future business plans, including those related to digital transformation.

Protiviti is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

CONTACTS

Jonathan Wyatt
Managing Director
The Shard,
32 London Bridge Street
London
SE1 9SG
United Kingdom
+44 (0)20 7024 7522
jonathan.wyatt@protiviti.co.uk

Ryan Rubin
Managing Director
The Shard,
32 London Bridge Street
London
SE1 9SG
United Kingdom
+44 (0)20 7389 4360
ryan.rubin@protiviti.co.uk

Hernan Gabrieli
Managing Director
Via Tiziano, 32
Milan
Italy
+39 02 6550 6301
hernan.gabrieli@protiviti.it