Information Security Forum

EU DATA PROTECTION REGULATION

COMPLIANCE GOES GLOBAL

The EU Data Protection Regulation will have an impact around the world. Organisations that act now can have a competitive advantage.

Over 80 per cent of ISF Members[1] either:

- operate from within the EU
- do business with organisations in the EU
- store data in the EU.[2]

These ISF Members are likely to handle (collect, process, exchange, store and discard) EU residents' data and will therefore be impacted by the EU Regulation.

Large amounts of personal data now circulate around the globe – often collected, bought and sold with few restrictions and minimal oversight. Individuals are realising that their data are valuable, but they have limited control over how it is used. This realisation has come as data breaches regularly expose sensitive details, and as websites and social media are shown to be gathering personal data. Public awareness has also been heightened by the Snowden revelations, which exposed large-scale personal data collection by numerous governments.

A **Regulation** is a binding legal act that is applicable in its entirety across the EU.

A **Directive** is a legal act that is transposed into the national laws of member states. It obligates states to achieve a result without proscribing the means of achieving that result.

Over the past 20 years, the internet and digital technologies have become an integral part of modern life and protection of personal data is now a widely shared concern.

The EU is worried that lack of trust will make people hesitant to use online products and services and this in turn could slow the pace of digital innovation.

The EU believes the current regime – the 1995 Data Protection Directive – is in need of modernisation.[3]

National approaches to implementing, auditing and enforcing the 1995 Directive vary widely between member states, creating confusion and an uneven playing field for data protection across the EU.[4] In response, in January 2012, the EU proposed a two-part reform:[5]

- A General Data Protection **Regulation** (GDPR) whose primary goal is to harmonise protection of personal data across all EU member states. It will replace the 1995 Directive and will apply across all business types and sectors.
- A General Data Protection **Directive** on protecting personal data processed for the prevention, detection, investigation or prosecution of criminal offences.

The Regulation is of particular interest to ISF Members and is the focus of this paper. Once approved, it will become law in all member states. It will have an international reach, affecting any organisation that handles the personal data of EU residents.

This paper clarifies the fundamental aspects and implications of the Regulation and provides recommendations. Action taken now can provide an advantage over those that are less prepared.

1 This figure includes all ISF Members in the EU and European Economic Area countries, as well as selected Members around the world that are deemed likely to handle personal data from EU residents.
2 Ben Rossi, "Countdown to the EU General Data Protection Regulation: 5 steps to prepare", *Information Age*, 24 March 2015, www.information-age.com/it-management/risk-and-compliance/123459219/countdown-eu-general-data-protection-regulation-5-steps-prepare
3 "EU Data Protection Directive Changes", *Optanon*, 16 May 2013, www.eudataprotectionlaw.com/changes/
4 Steve Wright, "The challenges facing cross border e-discovery", *Cyber Security Law & Practice*, May 2015, www.e-comlaw.com/cyber-security-law-and-practice/article_template.asp?Contents=Yes&from=cslp&ID=19, p. 14.
5 Press Release, "Data Protection Day 2014: Full Speed on EU Data Protection Reform", *European Commission*, 27 January 2014, europa.eu/rapid/press-release_MEMO-14-60_en.htm
6 EU law, "Regulations, Directives and other acts", *European Union*, europa.eu/eu-law/decision-making/legal-acts/index_en.htm, Accessed 26 May 2015.

Key aspects of the Regulation

The Regulation aims to establish the same data protection levels for all EU residents and clarify blurred lines of responsibility. It will have a strong focus on how organisations handle personal data. Organisations face numerous challenges in preparing for the reform, including a lack of awareness among major internal stakeholders such as legal, HR, information security and compliance. Many organisations are clearly not prepared for the Regulation and in some cases are unfamiliar with the fundamentals, as demonstrated by a November 2014 survey of 104 IT professionals in the UK (see Figure 1).

FIGURE 1: Are organisations prepared for the General Data Protection Regulation (GDPR)? [7]

73% **didn't know when the Regulation was due to come into effect.**

63% **admitted to having no idea what 'GDPR' stood for.**

The final draft of the Regulation is still being negotiated, but it is expected to be approved in spring 2016. The broad objectives remain focused on protection of personal data.[8] Once approved, organisations will have a two-year transition period to adapt to the new rules. To build and maintain popular support for this reform, the EU has emphasised the benefits to individuals, including:

A right to be forgotten:

When EU residents no longer want their data to be processed and there are no legitimate grounds for retaining it, the data must be deleted. The burden will be on the organisation, not the resident, to prove the data should be retained.[9]

Easier access to data:

A right to data portability will make it easier for residents to transfer personal data between service providers.

Allowing residents to decide how their data are used:

When consent is required to process a resident's data, they must be asked to give it explicitly.

The right for residents to know when their data has been hacked:

Organisations must notify their national data protection authority (DPA) of serious data breaches as soon as possible.

Data protection first, not an afterthought:

Privacy by design and privacy by default will be essential principles, although the specifics of implementation remain vague.[10]

The intention is that the reform will benefit both a generation that has witnessed the change from analogue to digital, as well as a younger generation that has only experienced the digital domain and has grown up being encouraged to share their (often poorly secured) personal data online.

These benefits will create numerous compliance requirements, from which few organisations will completely escape. However, organisations will benefit from the EU-wide consistency introduced by the reform and will avoid having to navigate the current array of often-contradictory national data protection laws. There will be international benefits as well. Countries in other regions are devoting more attention to data protection and the Regulation has the potential to serve as a robust, scalable and exportable regime with the potential to become a global benchmark.

Recent drafts of the Regulation have adopted a risk-based approach, which is premised "on the concept that compliance obligations should be proportional to the specific processing activities".[11] This stance offers welcome flexibility for organisations, though there are concerns that it could weaken data protection rights at the individual level if too much discretion rests with organisations.[12]

The EU has recognised the need to make the Regulation adaptable to changing technology – and to do this in a way that encourages innovation and offers commercial opportunities and benefits. This links closely to the EU Digital Agenda initiative, which aims to encourage innovation and develop a digital single market.[13] In areas where technology has advanced significantly in the past two decades such as social networks and cloud computing, the Regulation aims to clarify responsibility for the data organisations handle and store, thus making it easier for EU and non-EU organisations to comply and avoid fines.

7 Press Release, "European IT Teams Woeful Lack of Preparation for General Data Protection Regulation (GDPR) May Mean Painful Compliance Audits Ahead", *Ipswitch*, 12 November 2014, www.ipswitchft.com/about-us/news/press-releases/2014/11/gdpr-may-mean-painful-compliance-audits-ahead

8 Privacy & Information Security Law Blog, "Debate Over the Progress of the EU General Data Protection Regulation", *Hunton & Williams*, 2 February 2015, www.huntonprivacyblog.com/2015/02/02/debate-progress-eu-general-data-protection-regulation/

9 "Factsheet on the 'Right to be Forgotten' ruling (C-131/12)", *European Commission*, 2 June 2014, ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, p. 3.

10 Press Release, "Progress on EU data protection reform now irreversible following European Parliament vote", *European Commission*, 12 March 2014, europa.eu/rapid/press-release_MEMO-14-186_en.htm

11 Privacy & Information Security Law Blog, "Council of the European Union Proposes Risk-Based Approach to Compliance Obligations", *Hunton & Williams*, 29 October 2014, www.huntonprivacyblog.com/2014/10/29/council-european-union-proposes-risk-based-approach-compliance-obligations/

12 Privacy & Information Security Law Blog, "Debate Over the Progress of the EU General Data Protection Regulation", *Hunton & Williams*, 2 February 2015, www.huntonprivacyblog.com/2015/02/02/debate-progress-eu-general-data-protection-regulation/

13 Press Release, "A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen", *European Commission*, 6 May 2015, europa.eu/rapid/press-release_IP-15-4919_en.htm

Implications of the Regulation

Some of the main implications are related to data breach reporting, sanctions and fines, the one-stop shop initiative and global reach, each of which are described below. These topics also constitute significant points of disagreement (between organisations and member states on one hand, and EU governing bodies on the other) that remain under negotiation.

The EU is attempting to balance the competing priorities of encouraging a vibrant and innovative digital single market, while bringing member states to agreement on a far more stringent data protection regime. These two priorities are not always in conflict, as there is economic benefit to be gained from the efficiencies of establishing a global benchmark for data protection.

1 DATA BREACH REPORTING

The debate over breach reporting has been followed with significant interest by organisations. Varying time windows have been suggested by member states, with the most recent draft of the Regulation settling on 72 hours.

This would require the organisation to report a breach to the relevant DPA. In France, for example, the DPA is the Commission Nationale de l'Informatique et des Libertés. In Germany, it is both the Federal Data Protection Commissioner and the individual states, and in the UK it is the Information Commissioner's Office.

Reporting to DPAs such as these will be mandatory for breaches which are "likely to result in a high risk for the rights and freedoms of individuals" including:[14]

- discrimination
- identity theft or fraud
- financial loss
- breach of pseudonymity
- reputational damage
- loss of confidentiality of data protected by professional secrecy
- any other significant economic or social disadvantage.

Many of these risks are present in the majority of data breaches, although it is not yet clear how much guidance will be given to help organisations distinguish a high-risk breach from a low- or medium-risk breach. The current level of breach reporting in the EU is low (relative to the US) and the Regulation is likely to result in a soaring number of data breaches being reported to DPAs. Breaches not reported within 72 hours will have to be accompanied by a reasoned justification for the delay.

Compliance with these reporting obligations will place an administrative burden on organisations; however, there will be tangible efficiencies as well, including the benefit of having one breach response plan to cover all European operations.

If European breach reporting is effective there may be positive side effects in other regions. It could provide a constructive example for the US Government, which has struggled to pass a unified model for breach reporting and where organisations are confronted with dozens of competing state breach laws.

2 SANCTIONS AND FINES

The Regulation proposes a range of sanctions and fines for data protection violations to be levied by the DPAs, including:[15]

- a written warning (unintentional or first offences)
- regular and periodic data protection audits
- a fine of up to EUR 100 million or 2 per cent of annual worldwide turnover, whichever is greater.

These fines "mark such a significant departure from the existing regime that they constitute a conceptual change. Data protection will be as significant as antitrust in terms of compliance risk. Under the Regulation, data protection will no longer be an area in which businesses can afford to take casual risks." [16]

Depending on the size of the organisation, 2 per cent of annual turnover could significantly exceed EUR 100 million. Although a robust ceiling for fines should be expected, some member states have objected to fines being measured as a percentage. For some organisations, this amount is more than sufficient to erase profits.

Details of the proposals remain subject to negotiation. The 2 per cent fine was recently negotiated down from 5 per cent.[17] This is a welcome change although further revisions are possible.

14 EU Council, "Council's consolidated version of March 2015", *statewatch*, 21 April 2015, www.statewatch.org/news/2015/apr/eu-council-dp-reg-4column-2015.pdf, p. 344.
15 Ariane Mole, Ruth Boardman and Gabriel Voisin, "EU Data Protection Regulation: one step forward", *Bird & Bird*, 22 October 2013, www.twobirds.com/en/news/articles/2013/global/libe-committee-of-the-euro-parliament-votes-on-compromise-amendments-to-the-draft
16 "The Proposed EU General Data Protection Regulation – A guide for in-house lawyers", *Hunton & Williams*, April 2015, www.hunton.com/files/Publication/e148d184-7b15-4e62-b295-0febc750f64d/Presentation/PublicationAttachment/a04eeb85-4b86-4034-a7ca-1ed5c3f50c56/Hunton_Williams_EU_Regulation_Guide_Overview.PDF, p. 6.
17 EU Council, "General Data Protection Regulation – Chapter VIII", *statewatch*, 4 May 2015, www.statewatch.org/news/2015/may/eu-council-dp-reg-chap-VIII-8371-15.pdf, p. 26.

3 ONE-STOP SHOP INITIATIVE

The one-stop shop means that EU residents will deal with only one DPA for complaints that cover data protection issues anywhere in the EU. Likewise, organisations will deal with the DPA in the country of their main establishment.[18] The goal is to increase harmonisation and reduce the current fragmented environment in accordance with the EU's principle of subsidiarity, which ensures that decisions are taken as close as possible to the affected residents.[19]

"One-stop shop was meant to be a win-win-win approach to privacy compliance. Organisations would benefit from the consistency derived from being accountable to one single regulator, with whom they would interact and by whom they would be exclusively supervised throughout the EU. Regulators would delegate their international competence to whichever colleague was strategically best placed to do the job." [20]

For the one-stop shop initiative to succeed, DPAs across the EU need to function well within and between countries. Unfortunately, there are disagreements among member states as to the process for one regulator to delegate a data protection case to another regulator. Additional disagreements arise from how to prevent so-called forum shopping, where organisations base themselves in member states with less effective or less attentive regulators. Organisations can expect to see a complex mix of compromises emerge from negotiations on how best to implement the initiative.

4 GLOBAL REACH

Many organisations do not appreciate the extent to which the impacts of the Regulation will be felt beyond the EU. Its geographical reach will be significant and it will apply to organisations around the world if they handle personal data of EU residents, for example, when they provide services or track online activity. "This will apply to both [data] controllers and [data] processors – so US cloud providers who host personal data of EU [residents] will, in many cases, be directly subject to EU law – even when the cloud provider's clients are not themselves established in the EU."[21] Many organisations have not considered the need to communicate with supply chain partners, such as cloud service providers (see Figure 2) who may operate outside the EU.

FIGURE 2: There is a need to engage with critical suppliers (November 2014 survey)[22]

The same considerations apply to organisations headquartered outside the EU. **Any organisation interacting in some way with personal data from EU residents will be held responsible for its protection.**

Some organisations are making preparations but most are not. Suffice to say that the scope of the reform is large enough for it to be viewed as a global data protection law – and organisations are advised to begin preparations now.

18 Jan Philipp Albrecht, "EU General Data Protection Regulation State of play and 10 main issues", *The Greens/EFA in the European Parliament*, 7 January 2015, www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf, p. 3.
19 Summaries of EU legislation, "Subsidiarity", *European Union*, europa.eu/legislation_summaries/glossary/subsidiarity_en.htm, Accessed 28 May 2015.
20 Eduardo Ustaran, "One stop shop – Using tolerance to avoid forum shopping", *LinkedIn*, 29 September 2014, www.linkedin.com/pulse/20140929112434-24251273-one-stop-shop-using-tolerance-to-avoid-forum-shopping
21 Ariane Mole, Ruth Boardman and Gabriel Voisin, "EU Data Protection Regulation: one step forward", *Bird & Bird*, 22 October 2013, www.twobirds.com/en/news/articles/2013/global/libe-committee-of-the-euro-parliament-votes-on-compromise-amendments-to-the-draft
22 Press Release, "European IT Teams Woeful Lack of Preparation for General Data Protection Regulation (GDPR) May Mean Painful Compliance Audits Ahead", *Ipswitch*, 12 November 2014, www.ipswitchft.com/about-us/news/press-releases/2014/11/gdpr-may-mean-painful-compliance-audits-ahead

Recommendations

Some member states are better prepared than others. Some may have been motivated to implement the 1995 Directive aggressively, while others saw little benefit from updating their data protection policies. This disparity in maturity is one motivating factor behind the Regulation's two-year implementation period. If, as expected, it is approved in early 2016, then it will come into force in early 2018.

Organisations must consider in advance the steps they should take to prepare. The resources that may be needed – including time, people, policy and governance structures – will take time to agree and fund. There are actions that can help organisations get up to speed quickly, which will be beneficial regardless of last-minute amendments (e.g. changes to data breach reporting periods or fine percentages).

1 KNOW HOW DATA ARE HANDLED

The Regulation will impose new safeguards for data handling and the resource requirements for doing this will increase along with the sanctions and fines for non-compliance. Knowing how data are handled is an essential part of risk management. Organisations can begin by asking these questions:[23]

- What data are collected on EU residents?
- Where does it come from?
- What is it being used for?
- Where and how is it stored?
- Who is responsible for it and who has access to it?
- How much of the data held are still needed?
- Is it being passed on to any third parties?

Finding the answers to these questions will reveal a great deal about how an organisation uses data and the extent to which it permeates its business; it is also likely to reveal some surprises. It is to the organisation's benefit to uncover these before they come to the attention of a DPA. For example, inadvertently sending personal data outside of the EU could result in fines.

Some organisations have invested heavily in data security. However, even these are vulnerable to shadow IT (i.e. unsanctioned hardware or software that is introduced by employees, often in an effort to increase efficiency). Examples include flexible and free file-sharing tools such as Dropbox or Google Drive, which are often used to share data with colleagues or clients. Senior managers are advised to consider the added risk of shadow IT in light of increased fines that will result from data protection violations.

2 PREPARE FOR DATA BREACHES

Because of the effort required to report data breaches, it is essential that organisations prepare in advance. For many, this will require a more coherent incident response process along with closer cooperation between multiple departments, in particular legal. This coherence is essential, as DPAs will want to see a transparent rationale for remediation actions taken in response to a data breach.

The cost of non-compliance will increase, not only from new sanctions and fines but also from the court of public opinion. Reporting requirements will steadily push more data breaches into public view, creating reputational risks that many organisations have thus far avoided. Alternatively, organisations that establish themselves as trusted data protectors will benefit commercially.

3 DEVELOP TRANSPARENT GOVERNANCE

Some organisations may already have appointed a data protection officer to clarify internal data protection responsibilities, while others are waiting to see if this specialist skill will be mandated. This potential requirement has been the subject of much deliberation and the current draft of the Regulation remains vague, noting that "the [data] controller and/or the [data] processor may, or where required by Union or Member State law shall designate a data protection officer".[24] Based on previous drafts it seems likely that some internal oversight role will be mandated, based on the size of the organisation, the volume of data it handles, or the risks inherent in how it handles data.

"One of the key objectives of regulation is to cure bad behaviours in the economy. Putting it differently, if organisations had voluntarily adopted a culture of transparency, regulation would not have been necessary." [25]

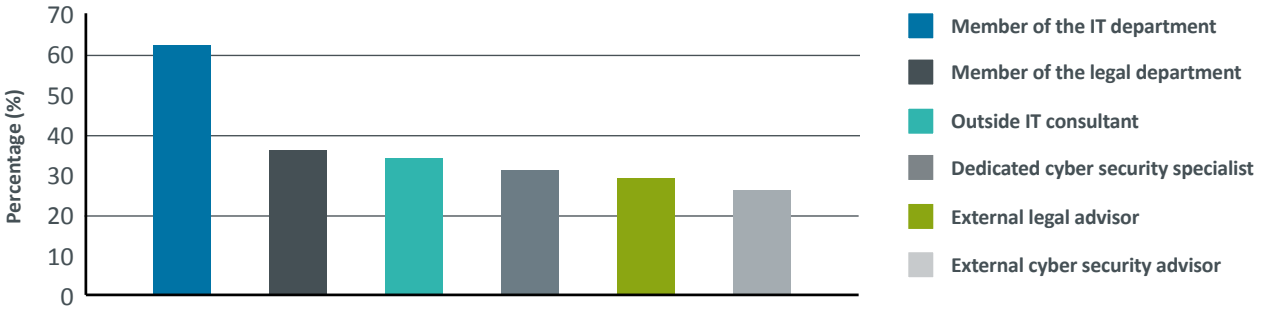
23 "Start Preparing for the DPR: Know Your Data", *Optanon*, 25 March 2015, www.eudataprotectionlaw.com/start-preparing-for-the-dpr-know-your-data/

24 EU Council, "Council's consolidated version of March 2015", *statewatch*, 21 April 2015, www.statewatch.org/news/2015/apr/eu-council-dp-reg-4column-2015.pdf, p. 375.

25 Stewart Room, "Are organisations burying the bad news?", *Cyber Security Law & Practice*, May 2015, www.e-comlaw.com/cyber-security-law-and-practice/article_template.asp?Contents=Yes&from=cslp&ID=14, p. 3.

Transparent governance and clear lines of responsibility will be key, as organisations will be required not only to identify the steps they have taken to protect data, but also to explain the rationale behind their decisions. This transparency will be essential when justifying actions to regulators. A January 2015 survey (see Figure 3) suggests that IT is the main department being held responsible for data protection planning, when in fact legal departments should logically share more of the burden, given the legal and jurisdictional complexities of the Regulation.

FIGURE 3: Who within your organisation will be assigned the tasks of assessing Regulation requirements and formulating compliance and reporting policies? [26]



Conclusion

The EU's goal of harmonising data protection regulations will introduce consistent and predictable safeguards across EU member states. The impact will be felt across the globe in all sectors.

The ISF suggests that the Regulation will apply to over 80% of ISF Members.

The Regulation is expected to be approved in spring 2016, followed by a two-year implementation period.

ISF Members that take steps now to:

- know how data are handled
- prepare for data breaches
- develop transparent governance

will have an advantage over those that don't.

ISF Members are encouraged to watch developments closely and join the ***Compliance Community*** on ***ISF Live*** (www.isflive.org/community/compliance) to share implementation experiences and learn from others' successes and failures.

26 A survey of 260 people working for organisations based in France, Germany and the UK, each of which employ over 500 staff. "Mixed State of Readiness for new Cybersecurity Regulations in Europe", *FireEye and IDG Connect*, 25 January 2015, www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/rpt-mixed-state-of-readiness-for-new-cybersecurity-regulations-in-europe.pdf

CONTACT

For further information contact:

Steve Durbin, Managing Director
US Tel: +1 (347) 767 6772
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

EU Data Protection Regulation: Compliance goes global
June 2015

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

CLASSIFICATION

Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.