General Data Protection Regulation and Episerver

Learn how to leverage your organization's data to support GDPR compliance.

What is General Data Protection Regulation?

What

The general data protection regulation (GDPR) is a new EU law that will come into effect on 25 May 2018 to replace the current Data Protection Act. It's the biggest overhaul of data protection legislation for over 25 years, and will introduce new requirements for how organizations process personal data.

The law applies to any company that is targeting consumers in the European Union and holding or transporting data relating to them, meaning it has the potential to impact companies globally, not just in Europe.

Episerver

At Episerver we have benefited from marrying our years of extensive experience and knowledge of cloud infrastructures and our already deep commitment to data protection, security and compliance. Through our internal policies, practices and track record, as we march towards ISO 27001 compliance, submit ourselves for Privacy Shield certification, over a decade of complying with German Data Privacy and Protection laws and our building of our Trust Center, including our industry-leading data processing agreements and processes, Episerver takes the GDPR pillar of data protection and privacy by design as a core principle moving forward.

With the implementation of the EU General Data Protection Regulation (GDPR) rapidly approaching, we at Episerver are happy to share some information on how our company is going through transformational changes to not just enable all of our Digital Experience Cloud customers to be best situated to get to GDPR compliance, but also be a leader in the Digital Marketing, Digital Commerce, Personalization, and Campaign field on all things GDPR.

This documents explains how Episerver is moving to GDPR compliance, and how our customers and partners can use the Digital Experience Cloud to quickly meet their own GDPR compliance requirements, as well as maintaining all of the functionalities and business requirements that drive their ability to become digital leaders.

We want to share some of our thoughts of ten high-level considerations customers and partners should have already started thinking about, as they move towards GDPR.

Peter Yeung
VP, General Counsel, Data Privacy Officer

1. Understand your organization's governance, then drive organization wide support

Get Executive Stakeholders

If your highest executive level sets privacy as a key priority, it sets the tone of privacy and compliance. Implement a privacy strategy or make a privacy mission statement. Involvement and support from executives will promote and push forward the compliance process, encouraging involvement and education of resources and assignment of tasks. Maintaining privacy and protection policies will dictate each organization's involvement in day-to-day operations.

We at Episerver have a Certification, Compliance, Security and Data Protection and Privacy Governance Board which the executive team and other key stakeholders participate in and holds regular meetings.

Get Key Individuals in Place

Once you get executive sponsorship, make sure you have a team of key individuals whom will drive the day-to-day execution of your data protection, privacy policies and governance. It is optimum to have each organization's participation. Another key member of a company's governance structure is the mandated Data Protection Officer (DPO). This is a key role under the GDPR and unless it is obvious that your organization does not need to appoint one an organization should document the reason for its decision.

At Episerver, we have both an Information Security and Data Protection Steering Committee, taking direction from the Governance Board, and have appointed a Episerver-Group wide DPO, as well as DPOs in various subsidiaries.

2. Understand your data and processing

One of the first tasks a company should undertake is a data mapping exercise in order to understand how data flows through your company. This includes the following key questions:

- What type of data is collected? Is it personal data?
- Who is collecting or using that data?
- Where is that data being collected, used, stored, and transmitted?
- When is it being collected, used, stored, and transmitted?
- How is it collected, used, stored, and transmitted?
- Why is it being collected, used, stored, and transmitted?

If you know the answers to these questions and map it out, you will understand the company's involvement in the collection, storage, use and transfer of data. This will enable your company to track the movement of data, and ensure that the data is correctly classified, have a thorough and ongoing record, and notify the relevant authority. Understanding this will also enable assessment of the legal basis for processing and ensure that the most appropriate processing ground is being used for each instance.

Some companies have invested in NIST's framework, ISO27001, ISO270018 or SOCII. If these frameworks have been implemented, that outputted work will advance your GDPR journey considerably.

At Episerver, as we have marched towards our own ISO certification, and implementing policies and practices NIST standards, we have and will continue to leverage our work there to accelerate our own GDPR journey.

3. Data privacy and protection are part of day-to-day operations

Under GDPR, companies have new legal accountability obligation to the law. As either data controllers or processors, companies need to demonstrate that such data control and/or processing occurs as the GDPR intends, requiring decisions and processing activities to be documented.

Data Protection and Privacy by Design

A key component of the GDPR is also data protection and privacy by design which means that data protection and privacy should be at the forefront of solutions, implementations and technologies the company is creating or implementing. This is another reason why it is important to have specific policies in place. Designers, architects, and developers should be assessing the data protection and privacy impact at the point of conception, creation or implementation, not on completion. Under GDPR, your company will need to document and justify why a privacy impact assessment (PIA) was OR was not carried out.

Protection, Privacy and Legal Considerations

Companies that have a clear and coherent process in place will benefit from the ability to assess, address, and react to privacy concerns early on. Your privacy and legal organizations need a seat at the table when innovation or development decisions are taken, and with your operations group when an issue occurs, as discussed later.

Accountability in other Departments / Organizations

Companies need to review all policies and procedures to ensure they instil privacy requirements, and where needed, updated to be compliant. This means aligning all policies including relevant information and contract retention policies, marketing policies, tracking/cookie/ analytics policies, consent policies, employee privacy policy, advertising practices, device policies, social media policies, hosting/operations policies.

As mentioned earlier, data protection and privacy by design is a core pillar in Episerver software development and managed services. We are reviewing and implementing new policies each week, having gap analysis done in each functional organization to ensure not just GDPR compliance, but also our drive towards being industry leaders in information security, privacy and protection.

4. Stay informed, learn and share with others

Clearly, it is not just your DPO, governance board or compliance committees that need to be informed and continuously learning. Companies benefit from creating iterative task specific training, legal and commercial updates and general privacy awareness. Companies in fact need evidence of this to show compliance with educational/ training aspect of GDPR, showing that resources and employees have a competent awareness of privacy laws applicable to their duties.

One of the obligations your DPO has is “awareness raising and training of staff involved in processing operations”. Other certifications and regulations, such as Privacy Shield, include obligations to train. Logically, you cannot teach everybody the law or all of GDPR, so condense GDPR principles for each organization, and duties as it relates to being a data controller and/or processor.

Episerver, through its DPO and Governance Board, drives on-going training, educational series and discussions around security, data protection, and privacy on an annual cadence. Meetings are also held with each functional group within Episerver based on GDPR, ISO and other regulatory/certification requirements, specific to that group.

5. Prepare for information security risks and events

To prepare for and mitigate any information security risks/ events all organizations within a company should have an information security policy which is updated regularly. You should ensure that you have clear steps and policies in place to protect personal data and prevent its loss. Encryption, pseudonymization, data-loss prevention strategy, restrictive access polices are a must. Here is another instance where ISO certification greatly help in achieving this. At a minimum, companies should align with a recognized security standard.

Through the ISO certification that Episerver companies have, and the ISO certifications that all Episerver companies are seeking currently, policies and procedures have been put into place and practice around these types of risk mitigation steps and policies.

6. Vendors, third parties, and others you should be talking to

GDPR obligations are not just relegated internally. Companies should ensure that data protection and privacy requirements are reflected in all contracts with third parties and that due diligence is always carried out. Be prepared to ensure the company has a policy or procedure in place to address non-compliance with regards to data protection and privacy. Regular reviews and updates of third party contracts should be carried out to ensure they reflect compliance with current privacy laws. It's proportional of course, for example, demands on your payment provider should be different from your facilities management vendor.

Episerver ensures that all applicable vendors sign an agreement that ensures data protection and privacy regulatory compliance, through such mechanisms as a data processing agreement.

7. Understand what notice and consent is, and make sure you get it

Companies must ensure that current communications and interactions with individuals at all points where data is collected, individuals are provided with appropriate notice and information as to the use of their information, including whether tracking and/or automated processing is used. In most cases under GDPR, consent is required, companies must also assess how that is obtained and evidenced. You should check that individuals can easily opt in and out, subscribe or unsubscribe to any emails or notifications, and ensure such mechanisms actually work. This is one of the biggest things data regulatory authorities will be looking for and paying attention to.

Episerver ensures that its own interactions follow strict policies on consent and opt-in/out procedures, and continuously reviews the effectiveness. Further, Episerver will publish best-practices in the future for customers/ partners, to help their own compliance on such.

8. Understand what an individual's rights are, and adhere to them

Under GDPR, individuals (known as data subjects) have many rights which they are permitted to execute at any time during their relationship with your company. To prepare for this, you should understand what requests you could receive at your organization and ensure there is a mechanism in place for dealing with such requests. They must be aware of their rights, easily request information from the company, and be able to request tasks such as "the right to be forgotten". FAQs, site instructions and dedicated communications (e.g. email) are useful to ensure individuals have the correct contact and how they can quickly assist with requests. Usually companies found in breach of data protection and privacy regulations are based on rights and protecting the rights of individuals – thus data subjects should always be forefront in any company decision making on communications and data subject interaction.

As you can see through our Privacy Policy, Episerver has clear instructions and methods for complying with data subject requests, as well as a clear model of gaining consent, and removing information if need be.

9. What happens when things go wrong? Plan on it

A management and operational plan, including a task force to be enacted, when a breach occurs is key. Having policies and procedures such as a notification system in place which works effectively, will benefit the company by ensuring that they stick to the time frames of reporting and resolution. Having a clear record of the steps taken by your company will also assist regulators and government authorities in helping you resolve the issue. Companies should keep a log of all breaches (or suspected breaches) and the investigation taken in each instance. Data privacy authorities will require this, and companies will benefit from these processes when conducting investigations into the cause of the breach, preventing a reoccurrence and provide an assessment of how the breach and recovery plan worked in practice.

Episerver's SIRT (Security Incident Response Team) has been trained and is ready to handle possible incidents that may occur. Further Episerver has put together policies and procedures company-wide, to assist the SIRT with the highest priority when assistance is requested.

10. An on-going commitment means on-going assessments

Above the penalties (which are significant) and guidelines that GDPR requires, at the heart of the regulation is corporate accountability. This is not a "one-and-done" exercise. GDPR compliance requires continuous review and updates, and inheriting the pillars as the corporate culture on an ongoing basis. Sadly, companies are never going to be "fully GDPR compliant" – it is an ongoing, living and adapting process which expects companies to constantly review, update and monitor the way data is handled.

Continuous testing and self-assessment of data protection and privacy policies are key to ensuring that the procedures will actually work, everything from a data subject access request procedure to an incident management plan. Keeping these up to date not just maintains your GDPR compliance, but ultimately reminds the individuals that your company interacts with a better, more secure experience.

As a final thought, GDPR compliance is a requirement which extends beyond assigning a privacy or compliance team, it requires the involvement and co-operation of the organization to take compliance with the GDPR from theory to practice.

Even those who have started with pushing through one of the first major tasks, data mapping, are starting to realize: it's one thing to have a core privacy team on top of GDPR, but a mammoth task operationalizing the GDPR throughout an entire organization. We at Episerver are here to help, show how Digital Experience Cloud is a key enabler of your GDPR journey, and are looking forward to going down the path together.

Remember -

IDENTIFY where your company currently is, data flows and what policies are already in place

REVIEW those existing policies, notices, processing grounds

ASSESS against GDPR compliance

UPDATE policies, plans, procedures, training, awareness to meet that compliance

TEST those policies through on-going audits and self-assessments

About Episerver

Episerver connects digital commerce and digital marketing to help organizations create unique digital experiences for their customers, with measurable business results. The Episerver Digital Experience Cloud™ combines content, commerce, multi-channel marketing, and predictive analytics in a single platform to work full-circle for businesses online — from intelligent real-time personalization and lead-generation through to conversion and repeat business — with unprecedented ease-of-use. Sitting at the center of the digital experience ecosystem, Episerver empowers digital leaders to embrace disruptive, transformational strategies to deliver standout experiences for their customers — everywhere they engage. Founded in 1994, Episerver has offices in Australia, Denmark, Finland, Germany, The Netherlands, Norway, Poland, Singapore, South Africa, Spain, Sweden, UAE, UK and the USA.

For more information, visit Episerver.com.