# GDPR

## 7 questions you should ask technology vendors about GDPR

# Introduction

When selecting a technology platform, it is important to consider how the vendor will help your organization comply with the European Union's General Data Protection Regulation (GDPR). The goal of this whitepaper is to help define what you should look for and expect from technology vendors regarding GDPR. The whitepaper will also explain how Episerver's Digital Experience Cloud can help you become GDPR compliant effectively and efficiently.

**Questions to ask technology vendors:**

1. Does the vendor have the right processes in place?
2. How will the vendor help you respond to data subject rights requests?
3. What support or processes does the vendor have in place to assist you with your data privacy impact assessments (DPIA)?
4. What has the vendor done in preparation for GDPR as it relates to their software and supporting services?
5. Beyond certifications, how detailed and tested is the vendor's security and compliance measures?
6. Does the vendor have the right people in place?
7. What has the vendor done internally to comply with GDPR?

# Your GDPR obligations for personal information

Technology platforms that interact with EU/EEA individuals must now comply with GDPR and all its data subject rights, responsibilities and obligations. This includes platforms for digital marketing, commerce and campaigns. It is not enough that a technology vendor ensures that their software platform and tools comply with GDPR, since your organization must also ensure that you use the technology in a compliant way. In particular, this involves how your organization controls and processes personally identifiable information (PII).

## Assessing your own risks and compliance measures

Please note that this whitepaper is not legal advice about GDPR, nor should any of the articles (such as the responsibilities around affirmative content, right to be forgotten, handling/processing of PII, acceptable technical and organizational measures, etc.), be used as a legal interpretation of any law or regulation. This is because each organization will be different in how they interact with data subjects, in how they are organized internally, and in what their business goals are. This means that your organization will be in the best position to assess your own risks and compliance measures as necessary.

Your organization should seek your own legal advice to fully understand the applicability of any law or regulation to your organization, including whether you collect and process PII yourself or through using Episerver or any other software company's products or services.

# 1. Does the vendor have the right processes in place?

Starting with the basics, you should ask if the vendor already has the right GDPR processes in place already. If they are still working on it, it's too late to get ready for the start of GDPR. Any GDPR-compliant vendor should be able to answer these questions quickly:

- ☐ Does the vendor have measures in place to ensure and demonstrate compliance with GDPR principles? If so, what are they?
- ☐ If the vendor uses external sub-processors (the vendor's processors), does the processing they carry out – and the contract under which they process your personal data – reflect these principles?
- ☐ Do you have specific technical and organizational security measures that you expect processors to comply with? Do current contracts under which processing activities are carried out meet the content requirements set out above?
- ☐ Have these been developed into a standard document/schedule? Does the vendor have a program for inspecting and auditing data processing to ensure that they are continuing to meet their guarantees and comply with their contractual obligations?
- ☐ Is there a clear obligation on the processor to maintain records of its processing activities and to cooperate fully with you and relevant supervisory authorities?
- ☐ Has the vendor (as a data processor processing personal data on your behalf) had due diligence exercises conducted to ensure that they offer sufficient guarantees that they will implement appropriate technical and organizational measures to process the data in accordance with the requirements of GDPR and the rights of data subjects?

According to GDPR, vendors (data processors) should have expert knowledge, reliability and resources to facilitate the issues addressed above. At Episerver, all of these questions are answered in our Trust Center, outlining our specific contracts, our global, technical and organizational measures across all products and services, and the methods in which we have conducted due diligence, not jtust within Episerver, but our with trusted sub-processors, such as Microsoft Azure™ and Amazon AWS™.

# 2. How will the vendor help you respond to data subject rights requests?

One of the biggest obligations organizations face under GDPR is responding to data subject rights requests (such as the data subject access, right to be forgotten, data portability, rectification, deletion, right to object, to restrict processing, to restrict automated decision-marking/profiling, etc.), which we group together as subject access requests (SARS). Vendors should not be deciding which SARS they can best respond to, but rather as a whole, explain how their software and services will provide SARS and support you in conducting them yourself. Questions to ask vendors include:

- ☐ Who within the vendor's organization is responsible for handing SARS?
- ☐ Does the vendor have procedures in place to respond to a SARS?
- ☐ What information does the vendor provide the data subject with?
- ☐ What exemptions does the vendor rely on currently when responding to SARS – either to redact personal data or to refuse a request entirely?
- ☐ Does the vendor charge for additional support in responding to SARS?

Episerver has dealt with SARS for more than a decade, even before they became a GDPR obligation. We have supported organizations globally with this issue through processes, resources and expertise in our managed services. In our continuing effort to improve, we have also augmented existing processes to facilitate faster responses and enable our customers and partners to execute and fulfil SARS themselves.

# 3. What support or processes does the vendor have in place to assist you with your data privacy impact assessments (DPIA)?

The obligations of doing DPIAs are not just for your vendors, but your organization as well. Questions you ask vendors about DPIA should focus not only on how they conduct internally facing DPIAs, but how they will assist you in conducting your own DPIAs. DPIAs are not one-off events, nor should they be considered a "line in a contract". They should be well-organized, thoughtful and – equally important – repeatable. Questions you can ask about this include:

- Does the vendor currently carry out privacy impact assessments? If so, when? Who carries out the privacy impact assessments?
- Does the vendor have procedures in place to classify the data you intend to process, based on the potential risk to the data subject, in order to assess whether a privacy impact assessment may be required?
- How would the vendor implement controls to ensure that an assessment is made for determining when new personal data processing needs to be subject to a DPIA before the processing commences?
- Does the vendor currently consult with data subjects or their representatives concerning the privacy impacts of proposed new processing that you are considering carrying out?

We at Episerver have conducted DPIAs for our internal systems, projects and processes that handle personally identifiable information (PII). We have also done them regarding our software and service offerings to our customers (including Episerver Digital Experience Cloud). In addition, we have a defined process and are ready to assist our customers and partners with their own DPIAs.

# 4. What has the vendor done in preparation for GDPR as it relates to their software and supporting services?

We will address the security, compliance and support measures further down, but first – how has the vendor prepared their software and supporting services to align with GDPR obligations? And furthermore, how have they adopted these principles of data privacy, protection and security as their core tenets and as obligations to their customers and partners? Beyond values and statements, what steps has the vendor taken to adopt these principles? Questions should include:

- What steps has the vendor taken to implement data protection by design?
- What steps has the vendor taken to realize the obligation to implement data protection by default?
- Does the vendor monitor, or regularly review, industry norms and new practices in respect to data protection and privacy?

At Episerver, we have built into our software and services encryption (where possible), pseudonymization techniques, while making processing more transparent. This enables customers and partners to monitor the processing of their data, as well as implementing data retention and destruction policies, and implementing DPIA methodologies in new and existing products that involve data processing. We have documented our best practices for both data protection by design, and data protection by default.

We have changed the default settings of our software and services to have these services turned on, as well as empowered customers and partners to manage and maintain privacy settings throughout. We ensure that any profiling, tracking and data collection must be thoughtfully activated by the customer and/or partner prior to their implementation, giving them an opportunity to review their practices and procedures prior to launch. You can find more information about this in our developer community, Episerver World.

# 5. Beyond certifications, how detailed and tested is the vendor's security and compliance measures? 6. Does the vendor have the right people in place?

Related to security, privacy and compliance, a starting point should be for the vendor to have certifications such as ISO 27001 or US-EU Privacy Shield, and the ability to provide SOC 1 and 2 reports. Vendors can say they have met GDPR obligations by having a data protection officer (DPO), and maybe even a chief information security officer (CISO), but do you know who they are? Do you know how qualified or trained their teams are? Here are some security and compliance questions you should be asking vendors:

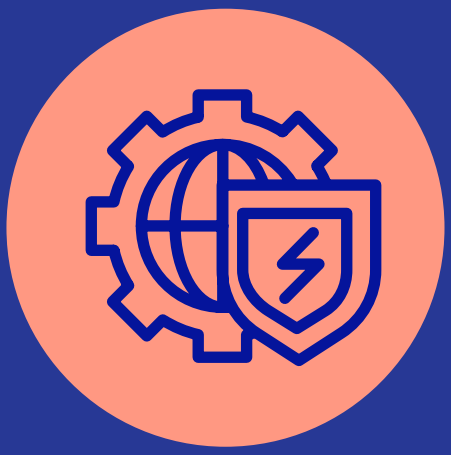
- Describe your information security compliance measures – meaning how many lines of defense do you incorporate across the software/services you offer?
- Please describe the governance boards and committees you have in place.
- What is your risk management methodology? How is your Incident Management Framework aligned?
- Who within your organization is responsible for the security of personal data? Does the role of this person cover manual as well as electronic records?
- Do you currently have a personal data security breach management policy and procedures?
- Who within your organization is responsible for handling personal data security breaches when they occur?
- Have you provided training to your staff on what to do in the event of a personal data security breach?
- Do the vendor's contracts with data processors require them to notify and cooperate with you in the event of a data security incident involving personal data that they process on your behalf?
- Does the vendor have a process for notifying the supervisory authority of a breach?

Episerver takes security, compliance, data privacy and protection as an everyday obligation, with each of our customers, partners, vendors and employees. We have done this by appointing a global DPO and CISO well before GDPR's obligations, by aligning teams across all organizations within Episerver, and by making significant investments in security and compliance processes, measures, and people (and their continuous training). In addition, with have more than a decade of experience in providing secure managed services. You can find more information in our Episerver Trust Center.

# 7. What has the vendor done internally to comply with GDPR?

What vendors do internally will give you good insight into to how they approach GDPR obligations externally, and into how much they understand GDPR principles and how seriously they take them. Some questions you should be asking vendors as it relates to their internal activities include:

- What steps has the vendor taken themselves internally (through sales, marketing, finance, human resources, research and development, ops, etc.) to ensure proper GDPR compliance?
- Did the vendor have to make any system and process changes to support GDPR? If so, what are they?
- How many staff have been trained on GDPR and data privacy? Which organizations have been trained? How often do those trainings happen?
- What GDPR steps has the vendor taken in regard to their own vendors and suppliers (not just the sub-processors they use with you)? Did they have to change their vendors based on GDPR?



## We're ready to answer your GDPR questions and help you

Episerver can answer all of these GDPR questions quickly and concretely. We have a long history of testing and adapting to privacy, security and compliance issues. We are not scrambling to make massive changes to our technology and processes because we have already prepared for these issues, years before GDPR became a reality. We are not constrained by the commercial implications of the increased obligations that data processors have under GDPR, and we continue to invest in our principles and structures around data privacy, protection, security and compliance. This puts us in the perfect position to help you.

## Contact Episerver for GDPR assistance:

Tell us about your GPDR initiatives and find out how we can help with them. We have a lot of information and expertise that we would be happy to share with you. Please contact your account executives or managers, or send an email to – sales@episerver.com. We'll answer your questions and walk you through your GDPR obligations, or put you in touch with our DPO and/or compliance teams.

## About Episerver

At Episerver, we believe digital transformation is a journey. We have been guiding customers for more than 20 years in providing standout digital experiences. Today our network of 880 partners, in 30 countries, supports 8,000 customers and over 30,000 websites. Founded in 1994, Episerver has offices in the US, UK, Sweden, Australia, Germany, Denmark, Finland, Norway, Poland, the Netherlands, Spain, South Africa, Singapore, Vietnam and the UAE.

## Episerver Digital Experience Cloud™

The Episerver Digital Experience Cloud™ unifies digital content, commerce and marketing in one platform, including omnichannel solutions for intelligent campaigns. The platform uses artificial intelligence and behavioral analytics to deliver personalized experiences everywhere. With our secure, reliable platform you can quickly increase engagement, revenue and productivity, while getting the fastest time to value.

For more information, visit episerver.com.

**www.episerver.com**