GDPR & Episerver Products

How Episerver's Digital Experience Cloud can help enable a customer's GDPR compliance.

The ever-closer march to May 25th, 2018

As the date of the European Union's General Data Protection Regulation (GDPR) comes ever closer, organizations which interact with EU/EEA individuals, their marketing departments, marketers themselves, and equally important - the individuals themselves (whom are the data subjects that the organizations are reaching out to), want to know what their rights, responsibilities and obligations are under GDPR.

Furthermore, it is important to know how the software platforms and tools that organizations choose, support their own GDPR compliance efforts, and meet those responsibilities and obligations, specifically around the control and processing of personally identifiable information (PII).

The goal of this whitepaper is to help define what the specific rights and responsibilities are for organizations, and how Episerver's Digital Experience Cloud can play a key role in enabling your organization to become GDPR compliant effectively and efficiently.

As always, 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 you and your organizations will be in the best position to assess your own risks and compliance measures as necessary. You and your organizations 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.

Not just "privacy by design" but "data protection by design" too

While some discuss how their platforms are designed and developed with "privacy by design", as required under GDPR, we at Episerver have taken this GDPR responsibility further. We have our software products and services go beyond data "privacy by design", and have engrained into the company ethos of Data Protection and Privacy by Design™. It's important at Episerver that in whatever we do, and however we operate, we keep as a core principle of doing what it takes to not just honor concepts around privacy, but protection as well.

We also have not executed Data Protection and Privacy by Design™ in a bubble – we have worked with many companies and organizations to date and we have extensive in-house knowledge in this domain, especially when it comes to General Data Protection Regulation (GDPR), ISO standards and the US-EU Privacy Shield certification process, collaborating with several parties and conforming to their standards and regulatory laws. This has enabled us to make Episerver the platform of choice when it comes to data privacy and security.

Below you can read some of the unique features of Episerver and how it helps secure sensitive information.

- **Data-at-rest encryption:** When data is stored in Episerver software services, we use data-at-rest encryption, further enhancing the security of PII data, drastically reducing risk of rogue actors ability to reach this data.
- **Secure transmission:** Data transmission across Episerver software services are sent over a secure channel, making tampering or monitoring difficult at best—greatly reducing intruders and potential "man-in-the-middle" attacks.
- **Encryption and Pseudonymization:** where possible, Episerver uses or allows customers to activate encryption throughout Episerver software services, and pseudonymization of PII is used throughout.
- **Extensive system audit logs:** There are more than 50 different system logs collected, and this helps system administrators and Episerver Operations and Managed Services teams know what is happening inside the cloud environment. In case of an emergency or an audit, logs can be viewed, allowing the organization to have insight into what has happened and the cause of issue.
- **Login security:** We have several methods to keep logins secure—Episerver can require strong passwords, only permit logins via HTTPS, and ban users when there is a brute force attack.
- **Storage location:** Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer's chosen region(s).
- **Access levels:** Episerver dashboard users can only view what has been enabled for them. Administrators have the ability to disable a menu item or a view (e.g User Profiles) for specific users. Customers manage access to their data and Episerver resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively.
- **Right to be forgotten:** If an EU citizen asks for his data to be removed, it can be completely wiped out in Episerver software services.
- **Do not track:** GDPR stipulates that individuals have a right to 'block' or suppress processing of personal data. If an individual decides not to be tracked, Episerver has a function to support this. If it is invoked, then users are not individually tracked at all.
- **Data portability:** Our database schema is completely open, allowing any Episerver client to transfer data from Episerver to another service easily. This can be done in a few ways, e.g. using command line or via API calls.
- **Self-hosting options:** Episerver can be installed on-premise (i.e. either in your own data center or with a trusted hosting partner), allowing for a greater depth and breadth of security and control. Self-hosting means that no third party (not even Episerver) ever has access to your data unless you permit it. When installed on-prem, the only stakeholder is the owner of the Episerver instance, hence the control.

Moreover, Episerver has modified our agreements available regarding GDPR assurance. Our data processing agreement (DPA) stipulates that customers can:

- Ask us to correct, amend or delete personal data.
- Ask us if there is a detect and report personal data breaches in a case.
- Ask us to demonstrate our compliance with the GDPR, e.g. regarding personal data collected.

Depending on the type of instance (cloud or on-premises licenses), chances are our customers can either follow the items above or get it done themselves.

Episerver Software Services and Data Subject Rights under GDPR

GDPR Article	GDPR Concept	Description	Episerver Enablement
Articles 1-4:	Scope	PII, Data Controllers and Data Processors defined with their roles and responsibilities, as well as singling out EU/EEA individuals	Episerver (as the Data Processer) enable customers (Data Controllers) to control where PII is stored.
Article 5:	Data Protection Principles	Ensuring PII is processed lawfully, fairly and in a transparent manner.	Episerver recommends that Customers ensure the use privacy statements accurately reflect the processing that they do, as Episerver shall process data as instructed by Customer.
Article 4(11): **Article 7:**	Affirmative Consent	Consent must be freely given, specific, informed and unambiguous indication. A statement or by a clear affirmative action, signifies agreement to the processing of personal data is required, and the controller must not simply obtain consent, but show and demonstrate through records kept for consent to be verifiable.	Episerver enables Customers to create forms and other information gathering techniques which will enable the proper, clear and affirmative consent needed. Further, Episerver suggests that Customers store that consent (and requisite information) properly in the Digital Experience Cloud database.
Article 12: **Article 13:**	Transparency and the right to be informed	If Customers process personal information, transparency about what it collect and how it uses it is mandatory. Transparency is typically achieved through privacy notices and privacy policies easily accessible to the data subject and can also be augment through other means.	Customers can create and publish their GDPR appropriate privacy policies and notice through Digital Experience Cloud, as well as develop further custom privacy settings, controls and preference centers.
Article 15:	Right of access by the data subject	Data subjects (individuals) are allowed to request a copy of personal data being processed so that they have the freedom to transmit it to another processing system if needed.	Digital Experience Cloud enables Customers to customize the access to their information stored, providing multiple options on getting information on data subjects back to them. Full access to the Digital Experience Cloud PaaS platform, including the database, means Customers have the flexibility to generate multiple access methods.
Article 16:	The right to rectification	Data subjects (individuals) are allowed to have their data corrected if inaccurate, incomplete, or wrongly contextualized.	Customers can, through Digital Experience Cloud, build forms, widgets and controls which gives the data subject access to correct their data themselves. Further, Customers can also facilitate corrections on the backend through their access of the system, including at the database level.
Article 17:	The right to erasure	Data subjects (individuals) have the right to request removal of personal data related to them on any one of a number of grounds, including cases where the fundamental rights of the data subject take precedence over the data controller's interests and require protection.	Digital Experience Cloud enables two specific methods of dealing which such requests. First, through Episerver APIs or through database access, Customer may execute irreversible deletion of such data upon request. Secondly, Episerver also supports the option to anonymize and aggregate such data, allowing Customer to retain the statistical nature of the data, but removing the possibility of having such data identifiable to a specific data subject.

Article 18:	The right to restriction of processing	Data subjects (individuals) have the right to restrict the processing of their personal data	Episerver offers Customer multiple ways through its entire suite of cloud solutions to enable this. With Episerver Campaign, Customers can and are advised to use the double opt-in functions pre-built into the service, as well as the opt-out features. With other Episerver software services, Customers will always have the option to customize the appropriate level of opt-in/opt-out, enable/restrict tracking, and enabling the affirmative consent required, whether its through exposed controls directly to the individual or through an internally managed process.
Article 20:	The right to data portability	Data subjects (individuals) have the right to request and receive any personal data a data controller or processor holds on them for their own use, or to port such data to another system and/or service.	Much like the request that may be made under Article 15, Digital Experience Cloud enables Customers to customize the access to their information stored, providing multiple options on getting information on data subjects back to them. Full access to the Digital Experience Cloud PaaS platform, including the database, means Customers have the flexibility to generate multiple access methods.
Article 21:	The right to object	There are rights for individuals to object to specific types of processing, including direct marketing; It is a right to opt-out of absolutely anything being done with an individual's data whatsoever to the extent done for direct marketing purposes, irrespective of whether that involves actually sending direct marketing to the individual.	Audit data protection notices and policies to ensure that individuals are told about their right to object, clearly and separately, at the point of 'first communication'; For online services, ensure there is an automated way for this to be effected; and Review marketing suppression lists and processes (including those operated on behalf of your organization by partners and service providers) to ensure they are capable of operating in compliance with the GDPR.
Article 22:	Automated individual decision-making, including profiling	Individuals have a right to not be subject to decisions made based upon automated processing, unless they provide explicit consent.	Digital Experience Cloud enables customers to build personalize experiences for end users, based on chosen information to collect and criteria to process. Industry best practices are to ensure transparency through easy to understand privacy statements and notice/consent language. Episerver platforms can help track and store information, however data processing decisions will always be the Customer's to make and implement.
Article 25:	Privacy by Design and Privacy by Default	Mandate that data protection protocols must be integrated into the business development process itself. All privacy settings must be set to high by default.	One of the core tenants of Episerver is awareness and embracing data protection and privacy in everything we do. Whether its building all software products and services with data privacy and protection by design, or ensuring that appropriate technical and organizational measures are taken in all infrastructure and support infrastructure, or inherent in all of our own internal processes and systems, privacy and protection by design and default is key in everything we do. Obtaining ISO27001 certifications, ensuring DPIAs are conducted, compliance and security structure through our CISO and governance groups and having a DPO and organization, are only a small subset of the internal and external activities at Episerver that support this ethos.

Article 30:	Records of processing activities	A data controller, determine the purpose of the data processing, describe that purpose. Additionally, record the types of people whose data are being collected, the types of data, duration of holding on, and whom it may be shared with (if any). Data processors must document the category of data being processed, sharing where such processing shall occur, and maintain the proper technical and organizational measures.	While Customers themselves will have to generate their own records for the "who, what, where, when, and how long" of the data they are controlling, Episerver itself has and maintains a data processing inventory, as well as snap-shot data inventory. Further, through the Episerver Data Processing Agreement ("DPA"), Customers are made fully aware of the categories of data being processed, where data is processed, and the technical and organization measures used. Digital Experience Cloud also includes robust and ongoing logging and reporting activities, which enable better on-demand information as needed.
Article 32:	Security of processing	To ensure that appropriate technical and organizational measures are taken for processing data, such as pseudonymisation and encryption of personal data	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Episerver implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk as the data processor, giving Customers a solid foundation to start fulfilling its requirements as data controller.
Article 33:	Data Breach notifications	Any case of data breach must be reported to the DPA by the controller within 72 hours of discovering the issue so that all parties involved can be warned about the situation and take precautionary measures.	Episerver has a well-established model for not just breach notification, but resolution, continuity and mitigation processes and models in place. Through the 3 levels of defense, the Information Security Management System (ISMS) group manages all arising situations on ISO standards, as well manages the resolution. Notice of such activities also given to the highest levels of management at Episerver.
Article 35:	Data Protection Impact Assessments ("DPIA")	DPIAs have to be conducted when anticipated and specific risks may occur regarding the rights and freedoms of data subjects.	Episerver conducts DPIAs on all of its software services and product lines, to ensure proper GDPR baselines are met. Further, Episerver also conducts DPIAs on internal processes and resources which involve the processing of personal data. Finally, when necessary and called to attention by the DPO, Episerver also conducts DPIA on specific projects where personal data risk mitigation is required.

Ready for Episerver? Ready for GDPR

Episerver wants to hear from you about your own GPDR initiatives and how we can help with them. We have a lot of information and expertise, and are always willing to share. Please feel free to contact your account executives or managers, or send email to – sales@episerver.com and we'll be happy to walk you through GDPR, or get you in contact with our DPO and/or compliance teams.

About us

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.