opentext™

White paper

GDPR compliance

GDPR preparedness with OpenText™ InfoArchive

The new EU privacy law, GDPR, will be in effect in less than a year. OpenText has the solutions to help you prepare and comply to this new law.

opentext™

Contents

opentext™

GDPR—General Data Protection Regulation: What's new? What's different?

The new law, which supersedes the 1995 Data Protection Directive, is a fundamental shift in the balance of data rights and obligations between EU citizens and businesses. The GDPR has new elements, including broader definitions of personal data and new rights for data subjects in terms of data portability, data erasure and higher standards for obtaining and managing consent. The 1995 directive was not a law but GDPR is, and it gives EU citizens significant control over their personal data. As a law, GDPR levies substantially larger fines for non-compliance on a global level since this regulation is focused on individuals and not territories.

Personal data—GDPR provides a broader definition of PII

Personally Identifiable Information (PII), a commonly used term in North America, refers to a relatively narrow range of data such as name, address, birth date, Social Security number and financial information such as credit card numbers or bank accounts. Personal data, in the context of GDPR, covers a wider range of information. The definition includes all tracking data that enables identification of consumers, such as Internet of Things IoT. Additionally, the concept of "indirect identification" of a data subject means that data gathered using cookies could be considered personal data. This indirect data provides context, relates to someone and can have an influence on the privacy rights of the person to whom it relates.

This aspect of context is important to understanding the GDPR. To make this tangible, think about a simple database. Imagine it only contains a list of first names, nothing else. If it's not fitting in a bigger context or cannot be traced back to someone, the list does not contain personal data but only an anonymous list of first names. But, when we add more context in the form of data, such as job function and surname relating to the first name, all the data elements, including the first name, are personal. Additional data sets that also provide context include social media posts, photographs, lifestyle preferences, transaction histories and IP addresses.

Privacy by design

Article 25 of the GDPR talks appropriately about "Data Protection by Design and by Default" and establishes that data protection must be built in to the functionality of systems. This has major implications for the entire process, from planning and product development to actual business operations.

By consolidating static information that contains personal information to a single repository, OpenText InfoArchive provides tighter security and controls, makes retrieval easier and reduces the risk of GDPR violations.

Among other things, this means that enterprises must:

- Have an overview of all personal data processing in their organization
- Provide data subjects with a list of their data
- Give data subjects the right to be forgotten/deleted
- Allow data subjects to transfer their data to other entities on request

Privacy by Design: When a new system or service is being developed and it will process or store data of EU citizens, the organization must be able to show:

- Appropriate security measures are in place to protect the data
- Continuous monitoring for compliance with GDPR throughout the lifecycle of the system or service

Are you agile enough?

Understanding how personal data is stored and processed across your entire digital ecosystem will likely require a deep assessment of your technology stack to determine whether your system is flexible enough to consistently obtain, track and accurately report on EU citizens/data personal information. Importantly, enterprises must analyze every application (legacy and production), device and database that processes direct or indirect identifiable data. Does your IT infrastructure have the agility to consistently manage EU citizen personal data across existing, legacy and future deployments? For example:

- Can you add attributes to transactional data and content to enhance context or minimize and pseudonymize data fields to protect privacy?
- Do you have a detailed audit trail that you can easily query to confirm collection, use and retention of personal information?
- Do you have accessibility functionality that allows self-service access for data subjects to view and download their personal data?
- Can you delete unnecessary data fields from transactional or IoT data sets after collection and analysis?

Do you have a comprehensive view?

If your customer and supplier profiles, personnel and HR records or transactional and reference data exists in silos—such as CIM, CRM and DMP systems—with no easy way to provide consistent access or retention and disposition policies, it is difficult to know if you're in compliance and easy to fall out of compliance without warning. It is also a challenge to fully understand complete personal information and perhaps impossible to erase personal data across the entire tech stack.

With data that is business complete, held for compliance or information governance purposes or as IP artifacts, it makes sense to place this data in a secured consolidated archive that can be easily accessed and provides the controls needed to adhere to the mandates of the GDPR.

Understanding GDPR compliance

Let's look into key considerations when assessing data privacy and compliance for the GDPR.

Where is the personal data that you control?

You should document what personal data you hold, whether it relates directly or indirectly to a data subject such as a customer, supplier, employee, contractor or even a job applicant. You should know where it came from, where it is and with whom you share it. You may need to organize an information audit.

How OpenText™ File Intelligence and InfoArchive can help

One of the most difficult tasks is identifying static content (static content or data does not change after being recorded) that exists on the various applications, file servers and devices in your organization. File Intelligence provides a powerful solution to identify, analyze and collect content in the wild. By simply scanning the IP addresses of systems and devices, File Intelligence can assess content that contains personal information. You can then act on the content–tagging, deleting, and collecting as needed. With visibility into to the business value and personal information contained in content, you can take appropriate action develop effective policies to meet GDPR requirements.

One of the most logical locations to move valuable or regulated, documents and data that contain personal information is to the InfoArchive platform. InfoArchive ingests data and content from multiple systems and maintains the contextual links created in the course of running the business. This provides the confidence, security, compliance and access needed to eliminate past applications and free up budget for modernizing your systems to better adhere to GDPR mandates.

The following section discusses critical articles in the GDPR and how InfoArchive can help you achieve compliance.

Understanding GDPR compliance and the information you manage

Article 7: Conditions of consent

7(1) Consent Documented

Businesses must provide records of the data subject's consent, including the conditions under which each data subject has given their consent, Terms of Service (TOS) and the specific purpose for which consent was obtained. Consent may be collected by different systems and in different forms. For example:

- When creating new accounts online: A data subject clicks a "Register now" button, creates a new account and clicks to accept TOS.
- When checking in as a patient at a hospital or a guest at a hotel or establishment: A data subject fills out a paper form that is later scanned into digital form to record TOS acceptance.
- When opting in or out: A data subject clicks into "My Account" and opts in or out of newsletters, events or other available options.

How InfoArchive can help

To manage evidence of consent across the data subject's lifecycle and multiple systems, InfoArchive ingests and stores registration transactions, forms, images and associated metadata that incorporate the intended use of data.

Article 12 (3): Transparent information, communication and modalities

Enterprises that manage personal data must respond to a request from the data subject without undue delay and in any event within one month of receipt of the request. If your information, both data and content is scattered across silos and not managed on a single platform, adhering to this timeframe will be difficult. If the timeframe is not met, the enterprise will be subject to substantial fines.

How InfoArchive can help

Enterprises use InfoArchive to manage all static data and content created and collected in the course of business operations and/or ingested from legacy systems. This information along with associated metadata is retained in accordance with applicable industry and territorial regulations. Since all the information is maintained in a single compliant and secure repository, requests can be met well within the one-month timeframe.

opentext™

Article 15: Right of access by the data subject

EU data subjects must be able to view and export personal data in commonly-used electronic format at any time. Also, data subjects have the right to be provided with information about all personal data stored by the applicable businesses.

How InfoArchive can help

Enterprises that employ InfoArchive can enable their data subjects to view and export their personal data via profile screens or secure web portals. This includes all static data and content ingested by InfoArchive from legacy and production applications and DMPs.

Article 17: Right to erasure ('right to be forgotten')

Data subjects have the "right to be forgotten"—that is, have their personal data erased by the enterprise, for reasons that include:

- The information is no longer necessary to fulfill the purposes for which it was originally collected
- The data subject withdraws consent for the business to perform the activity for which the processing is based
- The data subject objects to the purpose for personal data processing and the business cannot provide compelling, legitimate grounds to continue doing so
- The data subject's personal data was collected or processed unlawfully
- The data subject's personal data must be erased in order to comply with a legal obligation of that person's country of origin

How InfoArchive can help

The compliance controls inherent to InfoArchive provide enterprises with the controls necessary to not only meet this GDPR requirement but also ensure the demands of overlapping industry regulations are met. With InfoArchive, erasure of data can be scheduled. But if this conflicts with an industry regulation that the data be held for a determined amount of time, it will not be deleted until the period has been exceeded. This reduces risk and ensures that mandates are met.

Article 20: Right to data portability

The right to data portability requires enterprises to provide personal data to the data subject in a commonly used format and, if requested, to transfer that data to another controller if the data subject so requests. The right to data portability applies only when processing of personal data was originally based on the user's consent or on a contract. It does not apply to processing based on a public interest or the controller's legitimate interests.

How InfoArchive can help

InfoArchive has the ability to create a collection of data and then export that data in a commonly-used format, CSV, PDF, and others. The data can also be transferred to another controller. The data that is transferred will then be deleted if industry regulations allow. Otherwise, the information will be retained and deleted in accordance with the predominant regulation.

Article 28 (3)(G): Deletion of inactive data

The GDPR requires that businesses purge a data subject's personal data if the data subject requests or if the data subject has been inactive for a predetermined amount of time. All copies of such data must be purged as well, unless otherwise specified by law.

How InfoArchive can help

When a data subject's account has been inactive for a predetermined amount of time or if a data subject requests erasure, that data will be purged from the InfoArchive platform after a contractually mandatory time period that can be entered into the retention schedule. This erasure will take place unless predominate EU or Member State regulation requires longer retention of the personal data

Conclusion

The GDPR could result in a big overhaul of data privacy. It is a technological challenge because companies must develop the have policies and procedures, and most importantly, be able to carry out these policies through the prudent use of existing and new technology.

It will be difficult for organizations to identify, examine and manage personally identifiable information and consider how to comply with GDPR and the new data owner, the EU citizen. Taking into consideration GDPR Article 25, which states "you must implement appropriate technical and organizational measures for ensuring that, by default personal data which are processed and collected for the extent of their processing or the period of their storage/retention and their accessibility is protected and the rights of data subjects are meet," a consolidated repository should be part of any GDPR strategy. Time will prove that organizations that consolidate much of their data in one place and eliminate unsecured, unprotected legacy systems will be in a much better place.

The process of complying with the GDPR is going to be a challenge but enterprises should see it as an opportunity and use GDPR as a budgeted event. Use it as a catalyst to deploy more secure and modern solutions. Organizations should get educated and use this new law as a chance to strengthen and protect one of an organization's greatest assets–data.

About OpenText

OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

opentext.com/contact