



SINGLEVIEW FOR GDPR

**QUICKLY IMPLEMENT
DEMONSTRABLE COMPLIANCE**



In theory, 100 percent of businesses would be compliant with the European Union's General Data Protection Regulation (GDPR). In reality, that's not the case.

Before GDPR went into effect in May 2018, only 15 percent of businesses said they expected to be fully compliant, and 50 percent said they expected to have major gaps after its launch.

For businesses that collect and store vast volumes of data, such as sensitive billing information, it's not enough to be "half-compliant." You must know where all personal information is stored in your systems—and what steps to take to make sure you're fully compliant.

With Singleview for GDPR, we'll help you map out the steps you need to take on your GDPR journey.

SINGLEVIEW FOR GDPR

Singleview for GDPR is a complete service and solution, designed to offer data protection out-of-the-box to comply with GDPR and reduce the risk of fines and loss of reputation. To ensure you are fully compliant, we begin with an assessment of your Singleview implementation, followed by a strategic plan of the changes you need to make to demonstrate compliance.

First, our professional services team will work with you on a **GDPR Impact Assessment**. This is a complete inventory of information currently being collected, how consent is being managed, and what business processes you have in place. Together, we will look at what personal data Singleview holds, the legal basis for processing each category of data, data retention policies, and consent for data processing.

CATEGORY OF DATA	DATA ELEMENT	SOURCE	WHERE DATA IS STORED IN SV	PURPOSE	LEGAL BASIS	DATA PROTECTION REQUIRED	RETENTION POLICY	DISCLOSED TO THIRD PARTY
Customer, contact, order, usage, payment, etc.	What personal data is processed? (name, address, etc.)	Customer, third-party usage, etc.		Why is data processed? (order fulfillment, invoicing, etc.)	Performance of contract, legal obligation, consent, etc.	Encryption, masking, etc.		Name of third party (i.e. collection agency)

Examples of personal data mapped



Once you've completed the GDPR Impact Assessment, the next step is the **Configuration and Documentation of Data Protection Measures**. Data protection features are a built-in functionality of Singleview, including encryption and masking of fields, security roles, data retention and archiving and auditing to provide an audit trail.

The configuration process will help you maintain records of:

- Access or changes to personal data
- Attempts to access encrypted data
- Changes to security configurations
- Login attempts, login and logoff times
- All administrator activities, including creating new users and the maintenance of user access rights

In the final step of the process, we'll work with you on an **Implementation of Consent Management and Right to Erasure**. We'll design a consent management feature that's specific to your business, including but not limited to consent check boxes linked to data processing activities, business logic and records that the data subject gave for consent.

We will also help establish data erasure criteria, support automatic anonymization of personal information and bulk erasure.

Finally, we will help you to respond to Data Subject Access Requests by implementing a mechanism to extract the categories of personal data being collected, the purpose of the data processing, the recipients to whom the data will be disclosed; APIs support the integration with other systems that need to retrieve this information from Singleview.

SINGLEVIEW 10.2

The latest version of Singleview, Singleview 10, offers the following core features supporting GDPR compliance:

- Consent Management – Providing the ability to capture consent
- Data Erasure—Providing the ability to anonymize personal data
- Data Encryption and Masking—Customers can choose to encrypt and/or mask fields within the solution
- Security by Role—Robust security functionality controls data access, form access, and read/edit capabilities
- Auditing—Audit records can be maintained to record data changes, access to any sensitive data (unencrypted, encrypted or masked), changes to security configuration, login attempts
- Data Erasure—Providing the ability to anonymize personal data
- Archiving—Data that is no longer useful or necessary (e.g., closed customer accounts) can be removed from the system through archiving
- Data Extraction and Reporting—Data can be queried, extracted, and formatted for delivery to external systems or reports

European countries may have been the first to standardize data protection regulations—but they won't be the last. Other countries are considering their own data protection legislation, and it's better to be ahead of the change than behind it.



ABOUT CSG

CSG simplifies the complexity of business transformation in the digital age for the most respected communications, media and entertainment service providers worldwide. With over 35 years of experience, CSG delivers revenue management, customer experience and digital monetization solutions for every stage of the customer lifecycle. The company is the trusted partner driving digital transformation for leading global brands, including Arrow, AT&T, Bharti Airtel, Charter Communications, Comcast, DISH, Eastlink, iFlix, MTN, TalkTalk, Telefonica, Telstra and Verizon.

At CSG, we have one vision: flexible, seamless, limitless communications, information and content services for everyone. For more information, visit our website at csgi.com and follow us on [LinkedIn](#), [Twitter](#) and [Facebook](#).