

# The General Data Protection Regulation: What It Means and How SAS® Data Management Can Help



# Contents

Personal Data Defined .....	1
Why the GDPR Is Such a Big Deal .....	2
Are You Ready?.....	2
Accessing and Identifying Personal Data .....	3
Analyzing Data Flows.....	3
Logging.....	3
Establishing and Managing User Access Rights .....	3
Managing Incidents .....	3
5 Steps to Help on Your Journey to GDPR Compliance .....	4
Step 1: Access .....	4
Step 2: Identify.....	5
Step 3: Govern .....	5
Step 4: Protect .....	5
Step 5: Audit .....	6
SAS®: Trusted Software, Unified Approach.....	6
Learn More .....	6

Lawmakers and citizens in the European Union (EU) have been fiercely protective of personal data and privacy for years. With the May 2018 adoption of the most sweeping privacy law to date – the General Data Protection Regulation (GDPR) – the rest of the world gets involved, too. No matter where your business is located – Miami, Mexico City or Sydney – you’re on the hook to comply with this regulation if you store or process any EU consumer data, such as customer or employee data. And you’ll need to be vigilant and rigorous in your efforts.

The digital age, bringing with it technologies like cloud computing and the Internet of Things, has heightened the intense focus on personal data protection. The GDPR is designed to ensure continued, stringent protection and enforcement – and to simplify the regulatory environment for global organizations.

The GDPR defines personal data broadly and puts the individual at the center of data protection. It gives every EU resident the right to know and decide how personal data is being used, stored, protected, transferred and deleted. Individuals have the right to restrict further processing and to request that all their data be erased (the “right to be forgotten”).

Under the GDPR, you must be able to prove that you know where personal data is – and isn’t – across all your systems and lines of business. You need to know who can access this data, as well as when and how they do it. You’ll have to diligently safeguard against breaches. If you experience a breach, you must notify authorities and consumers within 72 hours, then rectify any resulting issues.

To underline the gravity of personal data protection, the GDPR strengthens enforcement and increases fines for noncompliance. Any organization that does not comply could be fined up to US\$22 million, or 4% of its global annual revenue (whichever is greater).

## Personal Data Defined

Personal data is broadly defined by the GDPR as any data that allows for the identification of an individual, directly or indirectly. This includes things like name, address, birthdate or identification number, as well as IP address, location data and any type of pseudonymous data. This is a much broader definition of personal data than previous EU directives used.

## Why the GDPR Is Such a Big Deal

To remain compliant with the GDPR, you must have clear documentation and policies on how you handle personal data, including where it lives, how it's used and who is accessing it. But many organizations don't have a clear definition of personal data and may not know exactly where all their personal data is located at any given time. And most store duplicate data in various systems. So erasing data in one system doesn't necessarily mean that all data is erased in other systems or databases. Without full traceability, organizations may find it impossible to accommodate the rights of consumers asking for usage information, or asking to have their personal data completely erased.

Consider:

- **Personal data can be elusive.** Column headers don't necessarily reveal column content. Personal data might reside in free-text fields, unstructured data formats and web streams, or it could be hardcoded into interfaces of legacy systems. And don't forget context. On its own, personal data could be meaningless, but when it's pieced together with other personal data, it could be linked to a real person and become high risk.
- **Your efforts need to be ongoing.** The GDPR is not just a matter of fix it and forget it. With the GDPR, the less governed your data is, the harder it is to stay compliant. Personal data could be in new data stores that aren't yet cataloged. Systems may change to meet new market and consumer trends. And data is often migrated from one place to another. It's vital for your company's policies to govern all of this data so you can keep up.
- **The GDPR calls for an organizationwide focus.** Everyone in the organization who handles personal data needs to understand how the regulation applies to them. This applies to everyone from the data protection officer to the database administrator. Because when consumers withdraw consent, all of their personal data will need to be erased. Doing this could prove tricky if duplicate consumer data resides in various formats and systems.

## Are You Ready?

It's clear that complying with the GDPR will affect your entire organization. You'll need to rethink how personal data is handled from the source of origin to the point of consumption. You'll also need to consider whether your data management and data governance frameworks can support GDPR requirements. You may even need to hire someone who understands data privacy and knows how to apply the law. The GDPR even requires organizations to have a data protection officer in most situations.

To be compliant, you'll have to find, evaluate and categorize personal data in potentially thousands of databases. You may need to create new processes, or at least evaluate current processes to make sure they're sufficient. You'll need to have people, processes and tools in place so you will instantly know:

- Exactly what data you have about your customers and employees.
- Where all of that data is stored (including data in your backup systems).
- That you're lawfully keeping and processing the data.

### Challenges of Complying With the GDPR

From an internal standpoint, make sure you can answer these questions:

- What (exactly) is personal data?
- How do we identify our personal data?
- Do we control access rights as we should?
- Do we log user activity for every data store?
- Within our systems, do duplication and poor data quality make it hard for personal data to be erased and forgotten?

Ask these questions to see if you're prepared to prove GDPR compliance:

- Can we provide an overview of all our data sources?
- Do we know the risk level for each data source?
- Can we show a report identifying where personal data is located?
- Can we prove that appropriate data management/protection processes are in place?
- Do we have all the necessary documentation and audit trails?

It can seem overwhelming when you consider all the necessary people, processes, systems and compliance measures that need to be in place. If you're like many organizations seeking to remain compliant with the GDPR, you face several challenges.

## Accessing and Identifying Personal Data

Accessing and identifying personal data is not as easy as it sounds. Normal drivers may be able to access relational databases, but you probably also have unstructured or poorly structured data, including web logs and social media data. Even network drives where you store content like Excel files need to be accessed.

Simply uncovering all of your personal data – then identifying it – can be tedious and error-prone. Traditional sampling methods and manual processes may not be sufficient. Not to mention that developers may have to write new programs with complex logic. All in all, efforts to remain GDPR compliant can be daunting. They could even disrupt performance of your business-critical production jobs.

## Analyzing Data Flows

Being able to document and assess the risk involved in all your data collection, usage and processing activities is a big effort. It requires monitoring many different actions, processes and plans related to personal data storage and processing. And each step along the way needs to be documented.

## Logging

To meet logging requirements, you'll need to be able to document precisely how all your systems are used. And you'll have to know who is viewing personal data so you can ensure that no unauthorized users have access.

## Establishing and Managing User Access Rights

To set up and manage user access rights, you'll first need to determine exactly who should be allowed to use specific systems and data. Then you'll need to specify how access rights will be enforced. That entails thinking through situations like when an employee is transferred to another department or quits his job.

## Managing Incidents

Under the GDPR, you must report to authorities within 72 hours if data is lost or if a breach in personal data is detected. You must also show which procedures have been initiated to fix the problem.



SAS provides software and services for all phases of the data protection life cycle.

## 5 Steps to Help on Your Journey to GDPR Compliance

With its industry-leading solutions for data management and analytics, SAS can help you meet evolving data protection compliance demands. We recommend five steps to help make your compliance efforts more manageable.

### Step 1: Access

The GDPR states that organizations are responsible for ensuring physical access to all stored data that is accessible. SAS® can help you locate data across different systems and networks, identify personal data that's affected by the GDPR, then start categorizing all the different types of data you have. That includes data in unstructured or poorly structured formats like social media and web log data.

If you're required to segregate compliance processes from business processes, or if you simply want to avoid disruptions and performance, you can use SAS Federation Server to speed your efforts with personal data investigation.

## Step 2: Identify

Identifying the personal data your organization handles in multiple sources and systems can be tricky – but this is where SAS excels. With data analytics software from SAS, you can effectively search for and identify Social Security numbers, personnel records, medical records and much more. Use it to search for terms and references that will help clarify the nature of the data. SAS software can also help you extract personal data from structured and unstructured data sources, no matter where it resides.

Sophisticated algorithms can go beyond traditional sampling methods and manual processes to strengthen personal data detection. You can reduce false positives by using automated data quality filters combined with techniques that regularly search files or personal data content. A potential timesaver is the SAS Quality Knowledge Base. This prepackaged solution contains data quality logic and rules such as identification analysis, pattern matching and extraction.

## Step 3: Govern

Once data has been identified, you need to define clear roles and responsibilities and establish terms and definitions in a governance model. There must be a common ground of understanding across the organization about the definition of personal data, who in the organization has the right to access specific personal data, and for what purposes it can be done. Based on this common understanding, you can tie terms and definitions to actual data that was discovered in the identification phase. Then you can link business terms with IT definitions, creating consistency and clarity across the organization.

SAS Data Governance can help you set and enforce policies, and get a consistent view of your data. It gives guidance and context to your data, and provides a single environment for aligning business and IT, pinpointing problems and monitoring quality.

## Step 4: Protect

Once you've located all of your personal data and established a governance model, it's time to set up the correct level of protection for the data. There are three de-identification techniques that can be used for compliance with data protection requirements:

- Anonymization, which removes personally identifiable information from data.
- Pseudonymization, which replaces personally identifiable information in data.
- Encryption, which encodes personally identifiable information in data.

Protection of personal data is also about authenticating, authorizing, monitoring and auditing security for users who access personal data. It also means that you won't compromise the identity of the people whose information you process and store as your organization conducts analysis, forecasting, querying and reporting.

SAS technology is built with strong security capabilities that can help with these efforts. And SAS Federation Server includes a security framework that makes it simple for you to mask and encrypt content when needed.

## Step 5: Audit

In this final step, you can use reporting tools like SAS Visual Analytics to visualize data discoveries and create easy-to-understand reports that can be shared with auditors and employees. These reports show you the control measures applied to systems, as well as users within the systems. So you can easily see which types of data are being used throughout the organization.

## SAS®: Trusted Software, Unified Approach

Throughout your organization, SAS delivers a unified view of your data. Our superior detection capabilities let you search your entire network to locate personal data stored in varying file formats and traditional and emerging data sources – across different functions, operating systems, platforms, and proprietary and commercial systems. With SAS, it's easier to find the data that's needed – even if it's hidden within columns or text strings, or is mislabeled or identified only by context. So you can seamlessly manage logging, user access and encryption to ensure enterprise governance and compliance.

Remaining compliant with the GDPR may be your primary goal today. But keep the larger goal in mind. With a solid data strategy, and better data quality and governance processes, it's not just your GDPR efforts that will be rewarded. SAS helps users analyze all types of data effectively. The insights uncovered can provide a foundation for faster, better business decisions across the enterprise. So you'll be positioned for the next regulation that comes into play – and gain a competitive edge along the way.

## Learn More

To learn more about the SAS approach to the General Data Protection Regulation, visit: [sas.com/pdp](https://sas.com/pdp).



To contact your local SAS office, please visit: [sas.com/offices](https://sas.com/offices)

