What it takes to be GDPR compliant
Understanding the impact of GDPR

The European Union’s General Data Protection Regulation (or GDPR) is a regulation intended to strengthen and unify data protection for all residents and citizens of the European Union (EU). It regularizes data privacy laws across Europe to protect all EU citizens’ data privacy and reshapes the way organizations across the region and beyond collect and manage personal data.

On May 25, 2018, GDPR compliance became mandatory. So, what impact does this regulation have on your business? How does it change the way you collect and store—even define—personal data? What are the implications for your current processes and technology?

At ServiceNow, we’ve been working hard with our customers on GDPR compliance so we have some insight that can help you understand the effect this new regulation has on your business, your employees, and your customers—including steps you can take to simplify ongoing compliance.

Let’s take a closer look.
Note that Global Turnover is similar to Annual Revenue.
A European regulation with global reach

GDPR doesn’t apply to EU companies alone. Any company that hosts the personal data of EU citizens in its systems must comply. You might have data on customers or employees who are EU citizens. Or maybe you have that data from a third-party such as a vendor or partner. How you got the data or where it came from doesn’t matter. If you have it, you must comply with GDPR.

What constitutes “personal data”? The GDPR definition is broad. A sweeping definition combined with the extensive scope of regulations and the high fees for non-compliance can make GDPR seem like an overwhelming challenge. The good news: we have a solution.

A broader definition of “personal data”

You probably already comply with strict regulations designed to protect data such as Social Security numbers, medical information, and credit card numbers and their associated names and addresses. What makes GDPR different? Any data that can identify someone is considered personal data. A name, a photo, social media posts, IP addresses, employee email addresses—it’s all classified as personal data under GDPR and is subject to more stringent regulation and oversight.
Treating data differently: privacy by design

The GDPR regulations are specific and extensive, and compliance will probably mean making some changes. Unless you rolled out a completely new system in the last few years, you probably don’t have the capabilities in place to meet these new requirements for data privacy. And the challenges aren’t just technology-based. You also need to treat data in a fundamentally different way under GDPR. Here’s how:

Protecting data anywhere—and everywhere—you have it

Under GDPR, you must protect personal data everywhere it resides in your organization. That may sound simple enough, but it’s not unusual for different applications and systems to access personal data, and that data might be replicated through back-up systems and disaster recovery systems. You may share data across a range of systems in your enterprise, from financial systems to order processing and eCommerce platforms, service management call center systems, warranty tracking, social media sites, human resource applications . . . and the list goes on.

Historically, some companies have focused on securing the hardware that stores personal data rather than the actual data objects themselves. That approach isn’t enough for GDPR compliance. Companies must prove that they protect the personal data of EU citizens every place it exists and in every system and application that uses it.

Gaining—and regaining—consent

Individuals must explicitly provide unambiguous consent to the storage and use of their personal data—and they have the right to revoke that consent at any time. The request for consent must be clearly distinguished from other items, such as terms and conditions. And posting forms that are pre-checked by default to indicate consent is not acceptable.

If you used a pre-checked online form allowing customers to opt in to email promotions after placing an order, those permission records may now be invalid for anyone residing in the EU. If you’re in this situation, your Marketing team needs to start re-building their lists.

If an EU citizen decides to revoke his or her consent, you may have to remove their data from all of your systems. Locating a specific person’s records in every affected system—including all applications, stored back-ups, and cold records—is essentially impossible without automation. And automating this process will require tools specifically designed to work with your systems.

Enabling portability

Customers will have the right to transfer their personal data among organizations. Imagine that a customer wants to switch banks. Under GDPR, they can ask their current bank to transfer all personal data to a competitor bank, and the original bank must comply in a secure and timely manner. Most companies today just don’t have the processes and capabilities in place to make these transfers as required—but ready or not, the mandate is here.
Job Creation: Data Protection Officer

Ready to update your org chart?

GDPR requires companies that process any personal data for 5,000 EU citizens or more each year to hire a Data Protection Officer (DPO). Adding together customers, employees, vendors, partners, prospects, and any other relevant category, you can get to 5,000 pretty quickly. The DPO is a role that doesn’t exist in most businesses today and finding qualified people who are ready to be completely accountable for data protection is a cause for intense competition among employers. But as with getting the systems and processes in compliance, companies need to fill the DPO roles.
Sound the Alarm

If your organization suffers a breach that compromises the personal data of EU citizens, GDPR requires that you notify your designated supervisory authority within 72 hours. If you operate in multiple countries, you can designate one supervisory authority to receive all reports, even on incidents that occur in other countries. Even so, unless you have a solution designed to handle the requirement it can take a lot longer than 72 hours to alert authorities and provide them with intelligent information about what happened.
One of the critical parts of GDPR compliance is that companies must complete Data Protection Impact Assessments before processing the personal data of EU citizens. What does this involve? It documents compliance with the GDPR, and it must be completed every time processing is “likely to result in a high risk to the rights and freedoms of natural persons.” That scenario could include anything from processing credit checks by banks to building marketing profiles based on website traffic patterns or combining matched data from various sources. With some types of processing, frequent ongoing assessments are required to identify risks. The assessment will identify gaps between your current state and GDPR requirements. Once you achieve compliance, the assessments verify that you’re maintaining it.
The heavy cost of non-compliance

Before the GDPR, the fines for not adhering to many European data protection regulations were lower than the cost of compliance. That equation has changed dramatically. Companies that don’t comply with GDPR can pay fines as high as €20 million or 4% of global turnover/annual revenue. In other words, compliance can’t be an afterthought anymore.
The first step on your journey to compliance is to map IT services and assets. With ServiceNow we identify personal data and create an information asset which gets tracked similar to other assets. Once you have an information asset we can identify every place it exists, where it moves, provide reports about information assets, and easily remove a specific asset when necessary. We then embed GDPR compliance controls into your processes and identify dependencies across programs and services. When risks arise, the GDPR dashboard pinpoints them so you can quickly address through remediation. Reports specific to GDPR are built in based on real-time data so you can document and demonstrate that you’re in compliance.

With ServiceNow, enterprises can streamline compliance controls, enhance internal audit productivity, and monitor risk. The results are real-time visibility and improved productivity of security, compliance, and risk management operations.
Now on Now
What it takes to be GDPR compliant

About ServiceNow
ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multi-step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow is the cloud-based platform that simplifies the way we work. ServiceNow software automates, predicts, digitizes and optimizes business processes and tasks, across IT, customer service, security, human resources, and more, to create a better experience for your employees and customers while transforming your enterprise. ServiceNow is how work gets done.