Preparing your organisation for the GDPR:

What you need to know

In 2016, the European Union ("EU") enacted the General Data Protection Regulation ("GDPR"), a far-ranging piece of legislation that regulates how organisations collect, store, and process the personal data of EU individuals. The goal of the GDPR is to strengthen data protection, simplify international business regulations, and return control of private information to the average person.

But, becoming compliant with the GDPR won't be quick or cheap for most companies that process personal data of EU individuals.

According to a 2016 report by Egress Software Technologies, 87% of CIOs are concerned that their organisation's current information security policies are insufficient to comply with the GDPR's tough new requirements, and 73.5% of CIOs are committing to tightening up their data sharing practices in response.

A recent PwC Survey of American companies with an EU presence found that 77% of those companies plan to spend $1 million or more on GDPR compliance.

While the GDPR was adopted by the EU last year, EU Data Protection Authorities have stated that they won't begin enforcing the regulation until May 25, 2018. As the leader in Cloud Identity, Okta has followed the development of this regulation closely, and developed this guide to outline the key points and offer solutions to help your organisation get ready for the GDPR. There's still time to prepare before May 25, 2018—depending on your organisation, there may also be a lot to do before then.

The GDPR is a dense 88-page document, but this guide will outline key points that you may need to know to be ready for next year. For legal advice regarding your organisation's specific GDPR compliance needs, be sure to consult with your lawyer. This document does not constitute legal advice.

87% of CIOs are concerned that their organisation's current information security policies are insufficient to comply with the GDPR's tough new requirements

Table of Contents

What is the GDPR?

> GDPR stands for General Data Protection Regulation. It is a law intended to strengthen electronic privacy for all individuals in the EU while creating uniform regulations for member countries

The GDPR protects the privacy of all individuals in the European Union (“EU”) by creating uniform regulations for member countries relating to the free movement of personal data.

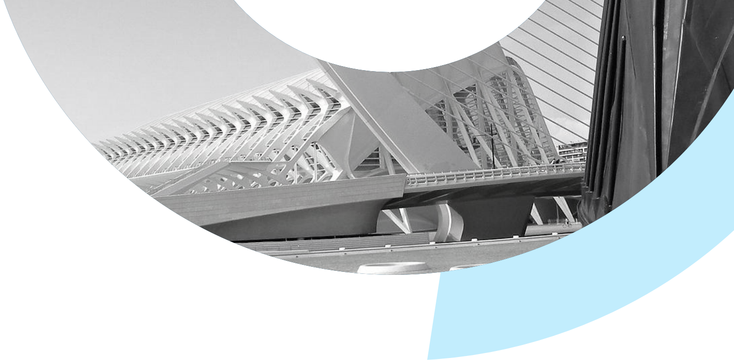
The GDPR applies to personal data created by citizens of the EU, but also puts new requirements on businesses globally that collect, store, and process the personal data of EU individuals, namely:

- Being able to quickly comply with erasure requests
- Making data more portable upon request

What data is regulated by the GDPR?

Some of the personal data regulated by the GDPR is fairly obvious, such as email addresses and employee ID numbers. It isn’t all so straightforward, though. The GDPR also regulates information that could be traced back to a specific person, so it covers geolocation and behavioural data that can be traced back to an individual, as well. The law was written to be future-proof, so it doesn’t provide a finite list of personal data types. Generally speaking, any data that identifies a living EU individual counts as personal data.

The GDPR goes further than past privacy regulations such as Safe Harbour and Privacy Shield by classifying an IP address as personal data, if it can be used with other data to identify an EU individual. This change in particular is a significant departure from previous privacy laws.



The history of the GDPR

The EU has been at the forefront of privacy law for a long time. In 1995, it adopted the Data Protection Directive, which broadly defined personal data as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”

This directive put the responsibility on public organisations to control data by taking into account seven principles:

1 Notice
2 Purpose
3 Consent
4 Security
5 Disclosure
6 Access
7 Accountability

Many privacy specialists believed that the directive was somewhat vague, and it left it up to each member nation how they intended to regulate personal data. This created roadblocks and confusion in international trade, leading to agreements such as Safe Harbour and Privacy Shield. These agreements attempted to provide a bridge between the privacy requirements of multiple countries, and were subject to many legal challenges regarding regulation harmonisation and the penalties for improper handling of personally-identifiable information (“PII”).

After some highly publicised lawsuits involving improper use of EU PII generating “slap-on-the-wrist” fines, discussion of the GDPR began in 2012 with the goal of creating a uniform data privacy law for the entire EU, while also expanding individuals’ control of their personal data.

When it was passed in 2016, the GDPR officially superseded the Data Protection Directive. While compliance isn’t mandatory yet, the penalties could be heavy for companies that don’t comply with it by May 25, 2018.

On this date, data protection authorities can begin levying penalties of up to 20 million Euros or 4% of a company’s annual worldwide revenue, whichever is greater. To avoid those potentially large penalties, organisations should take the time to prepare for the GDPR now.

Who does the GDPR apply to?

The GDPR applies to any global entity that collects, stores, or processes personal data of EU individuals. It classifies these entities as either data controllers or data processors. Speaking broadly, those categories can be defined as follows:

- A **data controller** exercises control over the processing of personal data, and decides which data to collect.
- A **data processor** acts at the direction of a data controller to collect, store, retrieve, or delete personal data.

In the vendor-customer context, Okta is considered a data processor under the GDPR, while our customers are data controllers. We will all be affected by the GDPR—we're in this together.

How will all of this impact you?

The biggest potential negative impacts of the GDPR are the possibility of fines, and the resulting erosion of an organisation's good standing in the eyes of its employees, business partners, customers, and other entities whose personal data it handles.

How can your organisation ensure it's compliant with the GDPR?

As of today, there is not yet a way for a third party to certify that your business is GDPR-compliant. Your legal team is the best source for advice on how compliance will affect your specific organisation. However, this guide can help you understand the key points of the requirements and some of the steps you'll need to take.

The first step is to understand what data the GDPR now regulates.

The most obvious part is **third-party data that includes personal data of EU individuals**—for example, personal data related to an organisation's customers or partners.

The GDPR also requires protecting **your own organisation's data that includes personal data of EU individuals**—for example, personal data related to your employees.

Essentially, any personal data of EU individuals that an organisation stores, collects, or processes for any reason falls under the purview of the GDPR.

Most companies just aren't prepared to handle that data in the way the GDPR requires. Some other information that could be regulated by the GDPR, depending on the facts of your use case, may include:

- Employee email addresses
- Information shared with wellness programme providers
- Business card printing records
- Organisation chart tools hosted by third party cloud providers
- Benefit tools
- Timesheets

While the scope of the GDPR can seem daunting, using an identity-as-a-service solution such as Okta can help companies better understand how they, and the third party services they use, handle, store and process personal data of EU individuals.

How ready are you?

> The right to erasure means an individual can request an organisation delete their personal data if it is no longer needed for its original purpose, they withdraw their consent, or have objections to how it is being processed

There's a lot to unpack in the GDPR, and the Article 29 Working Party, which is an EU organisation that assists with the regulation's implementation, is continuing to issue guidance to companies about the law's enactment and enforcement details. Still, there are several key points that any business can take into account now to help ensure compliance by May 2018.

Map your data flows

First, you'll need to know where any personal data of EU individuals in your control is going and which applications you use have access to it. This means mapping out your data flows with a visual representation.

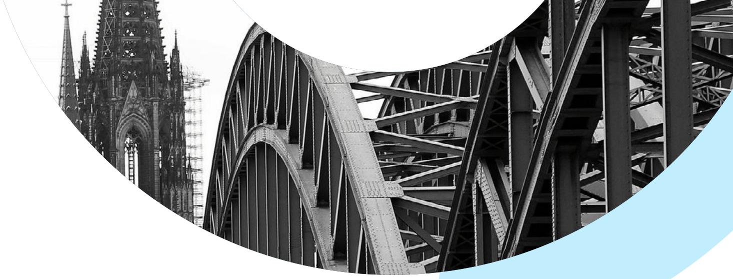
For example, are you keeping personal information about your customers and employees in Salesforce? Workday? How is it being used, stored, and processed?

Once you've figured that out and mapped it, you've likely done a good portion of the preparatory work that the GDPR requires. Ensure you're able to locate and erase EU individuals' data. Under the GDPR, EU individuals have broader abilities to request that organisations that store, process, and control their personal data delete that data.

The right to erasure means an EU individual can request that an organisation delete their personal data if:

- It is no longer needed for its original purpose
- They withdraw their consent
- They have objections to how it is being processed

This means organisations need to know exactly where that personal data is, including where any copies may be stored, so that it can be quickly deleted.



Be able to transfer personal data if requested

Another major GDPR requirement is the right of subject access and data portability.

An EU individual must be able to transfer their personal data from one processing system into another without interference from the data controller. The data controller also must provide this data to the individual in a commonly used open standard electronic format.

This is why it's so important for data controllers to have a map of their data flow. The map will make sure they know where personal data is being transmitted, which applications have copies of it, and what format it's in.

There are a lot of new requirements to evaluate, but remember that the first steps to becoming compliant with the GDPR are relatively simple.

> An individual must be able to transfer their personal data from one processing system into another without interference from the data controller. The data controller also must provide this data to the individual in a commonly used open standard electronic format

How Okta can help

> In 2016, the average employee actively used 36 cloud services. The average enterprise used over 1,400 cloud services

While Okta can't solve all the challenges presented by the GDPR, Identity and Access Management using a product such as Okta can provide a strong foundation for GDPR compliance and can help reduce your risk.

Remember that any other entity that handles your organisation's personal data of EU individuals, including vendors, partners, and apps, could add to your organisation's overall risk profile. Okta provides consolidation and visibility into the use of PII to meet security and compliance needs for both your enterprise and customers.

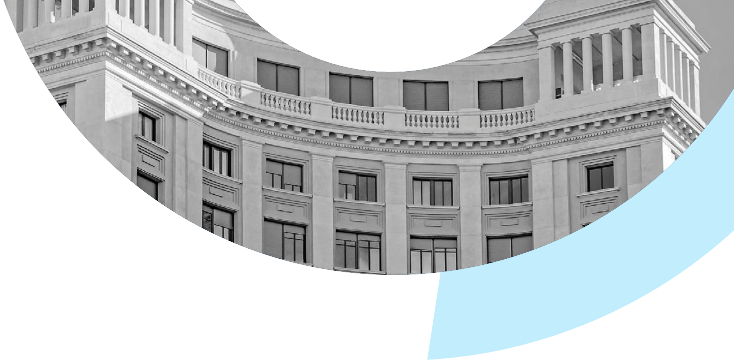
In 2016, the average employee actively used 36 cloud services. The average enterprise used over 1,400 cloud services. Are you aware of 1,400 applications being used within your organisation? Probably not.

But if each of those apps is loaded with the personal data of EU individuals, and if you receive an erasure request under the GDPR, you may be responsible for deleting the personal data across all those apps—no matter how obscure the app may be.

GDPR compliance can be a major undertaking, but Okta can help consolidate your business's identity management and provide greater visibility into this data. With Okta, you can easily find users in your Okta Universal Directory, and see which applications provisioned through Okta they have access to. That provides a good starting point for locating their personally-identifiable information.

Our platform helps both individual users and large enterprises ensure they're complying with GDPR requirements:

- **IAM for Enterprises** provides holistic security and compliance for employees and other partners that organisations work with. For example, Flex deployed Okta to their suppliers and employees.
- **IAM for Customers** provides end-to-end security and compliance for identities provided to customers. For example, Adobe's customer platform is secured through Okta.



A single source of truth provides visibility and eliminates identity sprawl

SSO

Okta Single Sign-On (SSO) provides a consistent login process with a single set of credentials. With visibility into all apps, SSO reduces identity sprawl and can provide for a single source of truth for right-to-be-forgotten deletion requests.

When News Corp first launched Okta, it was to one business unit for an initial trial. Within nine months, the company had deployed Okta to all of its businesses, successfully connecting 25,000 employees and more than 150 apps to the Okta platform with SSO. Dominic Shine, CIO at News Corp, says Okta "provided really good access to a very large number of applications and was clearly committed to ensuring that open access as the market developed."

MFA

Okta Adaptive Multi-Factor Authentication (MFA), also secures access to all apps and offers additional authentication factors based on the context of an authentication event.

For Funding Circle, the security benefits bring peace of mind: "Our business can go to bed at night and feel very, very comfortable that we have the right expertise and the right backend to support our applications' delivery," says Ayotunde Obasanya, Head of Infrastructure. Using Okta, Funding Circle's IT team can create robust access policies based on user data such as location, IP address, or device.

Universal Directory

Okta Universal Directory further secures personal data for employees, partners, and customers through its fully encrypted and unified user profiles. Scalable to support over 100M users, Universal Directory also offers the precision to identify and manage individual users, including the ability to remove users and their PII who are no longer with the organisation.

For ENGIE, Okta Universal Directory provides agility and simplifies processes for all M&A activity. It allows IT to synchronise data from various directories across the company. With all 100+ Active Directory domains connected to Okta, ENGIE consolidated users across all domains into a single Global Address list, making it much simpler to manage use of Office 365.

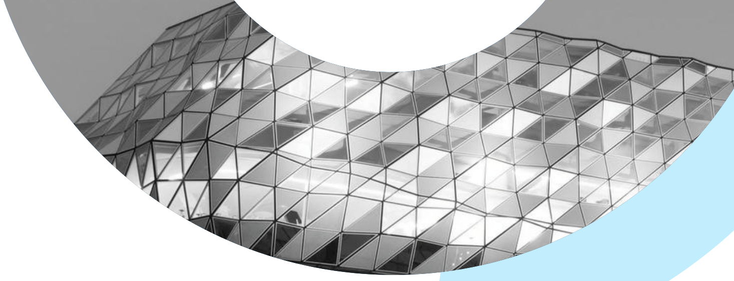
Lifecycle Management

Finally, Okta's Lifecycle Management provides unprecedented visibility into which users have access to which apps and their individual permissions. With reporting capabilities that can show both used and unused entitlements, as well as which identity attributes can be accessed by internal and external apps, organisations can use Lifecycle Management to build a holistic map of who has access to what data, a process critical to GDPR requirements. With visibility into all apps and how frequently they're being used, organisations can also decide whether they're adding value or aren't being used.

For Gatwick Airport, IT is critical when it comes to ensuring an efficient customer experience. Since choosing Okta, their productivity is up an estimated £700k. Okta's Lifecycle Management has also been beneficial for management, allowing for automated provisioning and preparing for audits. "Okta allowed management to perform mini audits ourselves to make sure all work was proceeding as we needed it to," says Michael Ibbitson, CIO.

Standards-based solutions support growth now and in the future

One of the most challenging components of the GDPR is the requirement to export PII in industry-standard formats upon request by the EU individual. Okta has been built on the concept that customers own their own data, and to that end, has always provided self-service access through APIs and standard reporting tools.



Real-time security alerts

Organisations' IT and security teams need visibility into their systems and actionable information. But if there's too much visibility, alerts that they can't act on, or not enough information available to them, there's a risk of fatigue.

This could be a significant problem under the GDPR, which requires that covered organisations inform the relevant supervisory authority within 72 hours of a data breach. If data has been exposed that may affect a consumer, organisations may need to notify them as well.

With Okta, you get real-time information about security issues—you don't need to wait for a request to get through a security team. You have all of this information right at your fingertips.

> The GDPR requires that covered organisations inform a data protection authority within 72 hours of a data breach

Next steps

Whether you're ready or not, the GDPR is coming, and the cost of noncompliance is high. However, preparing your business for the GDPR is a matter of mapping your data to be able to handle requests under the new regulation. And though that may sound like a tall order, partners such as Okta can help get you ready.

Looking for more resources to help your organisation prepare for the GDPR?

- Watch Okta's webinar on the implications of the GDPR
- Start your free 30-day trial of Okta