vindicia®
The Subscription People
An Amdocs Company

General Data Protection Regulation (GDPR) FAQs

Frequently asked questions about the European Union's new data protection regulations

Q. What is GDPR?

The General Data Protection Regulation (GDPR) is legislation of the European Union that regulates how personal data is managed. Personal data includes any information that can be used to directly or indirectly identify a person such as a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

The GDPR applies to companies in two broad categories: "controllers" and "processors." Controllers are companies, such as merchants, that collect personal data like credit card information and make decisions on what will be done with that data. Processors are companies that act on the behalf of controllers, storing and cataloguing that data.

The purpose of the GDPR, as defined in the press release, is to promote a Single Digital Europe, protect all EU citizens from privacy and data breaches, and enable people "to get back control of their personal data."

Q. When does GDPR go into effect?

May 25, 2018. The GDPR does not require any enabling legislation to be passed by government.

Q. Who does GDPR affect?

The GDPR not only applies to organizations located within the EU, but it will also apply to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

Q. How will GDPR affect businesses?

GDPR contains many requirements about how you collect, store, and use personal information. This means not only how to identify and secure the personal data in your systems, but also how to accommodate new transparency requirements, how you detect and report personal data breaches, and how you train privacy personnel and employees.

Q. A key purpose of GDPR is to protect personal data. What constitutes personal data?

Any information related to a natural person or "Data Subject" that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Q. How does the GDPR affect policy surrounding data breaches?

Proposed regulations surrounding data breaches primarily relate to the notification policies of companies that have been breached. Data breaches that may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

Q. What other rights does GDPR afford users?

The new user rights that GDPR legislates include:

- **Right to Access.** People (or "Data Subjects," as they are called in the regulation) have the right to obtain confirmation from the data controller as to whether their personal data is being processed, where and for what purpose. Further, they are entitled to receive a copy of the personal data, free of charge.
- **Right to Be Forgotten (or Data Erasure).** People can demand that the data controller erase their personal data and cease further dissemination of the data.
- **Data Portability.** People can receive the personal data concerning them, which they have previously provided, and have the right to transmit that data to another controller.

Q. Is Vindicia® CashBox® GDPR Compliant?

Ensuring security and privacy is part of Vindicia's DNA. We have always complied with all relevant legislation to ensure compliance with all security and privacy requirements wherever we do business, for example, EU model clauses and EU/US Privacy Shield (and previously EU Safe Harbor principles). For us, complying with GDPR is an incremental change only. Vindicia will be fully GDPR compliant before the requirements come into effect. Moreover, as the GDPR is still developing, Vindicia will meet new requirements as they arise.

Solution Brief

Q. What steps must companies take to become GDPR compliant?

For most companies, the fact that Vindicia CashBox complies is not sufficient for them to achieve GDPR compliance. Companies have to analyze the full impact of GDPR on their entire organization. This includes IT, marketing, data, legal and other departments that also may have to achieve compliance. Moreover, processes for managing personal data will also have to change.

Vindicia suggests that companies consider employing third-party consultants at least to assess the impact of GDPR, and maybe also to implement the necessary changes in systems and procedures. The classic system integrators and boutique consultants offer assistance with GDPR readiness. A simple Google search will find consultants in your area and industry.

Q. Which companies need to appoint a data privacy officer (DPO)?

Companies whose core activities consist of processing operations that require regular and systematic monitoring of people on a large scale (e.g., municipalities) must appoint DPOs. In the words of the regulations, "DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large-scale processing of sensitive personal data." DPOs must be appropriately qualified data experts. As the requirements are complex, it is advisable to consult a GDPR expert to understand if a particular organization requires a DPO.

Q. How will GDPR affect how businesses design software?

Two major requirements included in GDPR are:

- **Easy to Ask for, Give and Withdraw Consent.** Consent request and agreement must use clear and plain language. No legalese. Companies must be able to show that consent has been given. And it must be as easy to withdraw consent as it is to give it.
- **Privacy by Design.** Data protection must be included from the onset when designing systems. Controllers should hold and process only the data absolutely necessary for their needs (data minimization). Access to personal data should be limited to those needing access.

Q. How much will it cost to meet compliance with the GDPR?

Meeting compliance with the GDPR will cost time and money for most organizations, though it may be a smoother transition for those who are operating in a well-architected cloud services model and have an effective data governance program in place.

Q. What happens if a company is not GDPR compliant?

There are wide-ranging powers to impose penalties on companies that are not GDPR compliant. The penalties can be extremely severe. Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 million (whichever is greater). This maximum fine would be imposed for the most serious infringements, e.g., not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

Learn More about GDPR

- The EU GDPR website
- The full text of the regulations (216 pages)
- Microsoft Resources for GDPR compliance. This site has lots of information – white papers, blogs, FAQs
- International Association of Privacy Professionals (IAPP) has extensive info on GDPR preparations
- Three minute video by GDPR on the improvements in data privacy introduced by GDPR

US Headquarters
Vindicia, Inc.
2988 Campus Drive
Suite 300
San Mateo, California
94403-2531
P +1 650 264 4700
F +1 650 264 4701
vindicia.com/contact-us

ABOUT VINDICIA

Vindicia, an Amdocs company, offers comprehensive subscription management solutions that help businesses acquire and retain more customers. Providing much more than just a billing and payments system, the company's SaaS-based subscription management platform combines big data analysis, strategic consulting and proprietary retention technology. Vindicia provides its clients with more recurring revenue, more customer data, better insights, and greater value throughout the entire subscriber lifecycle. That's why they call us the Subscription People. To learn more visit **www.vindicia.com.**