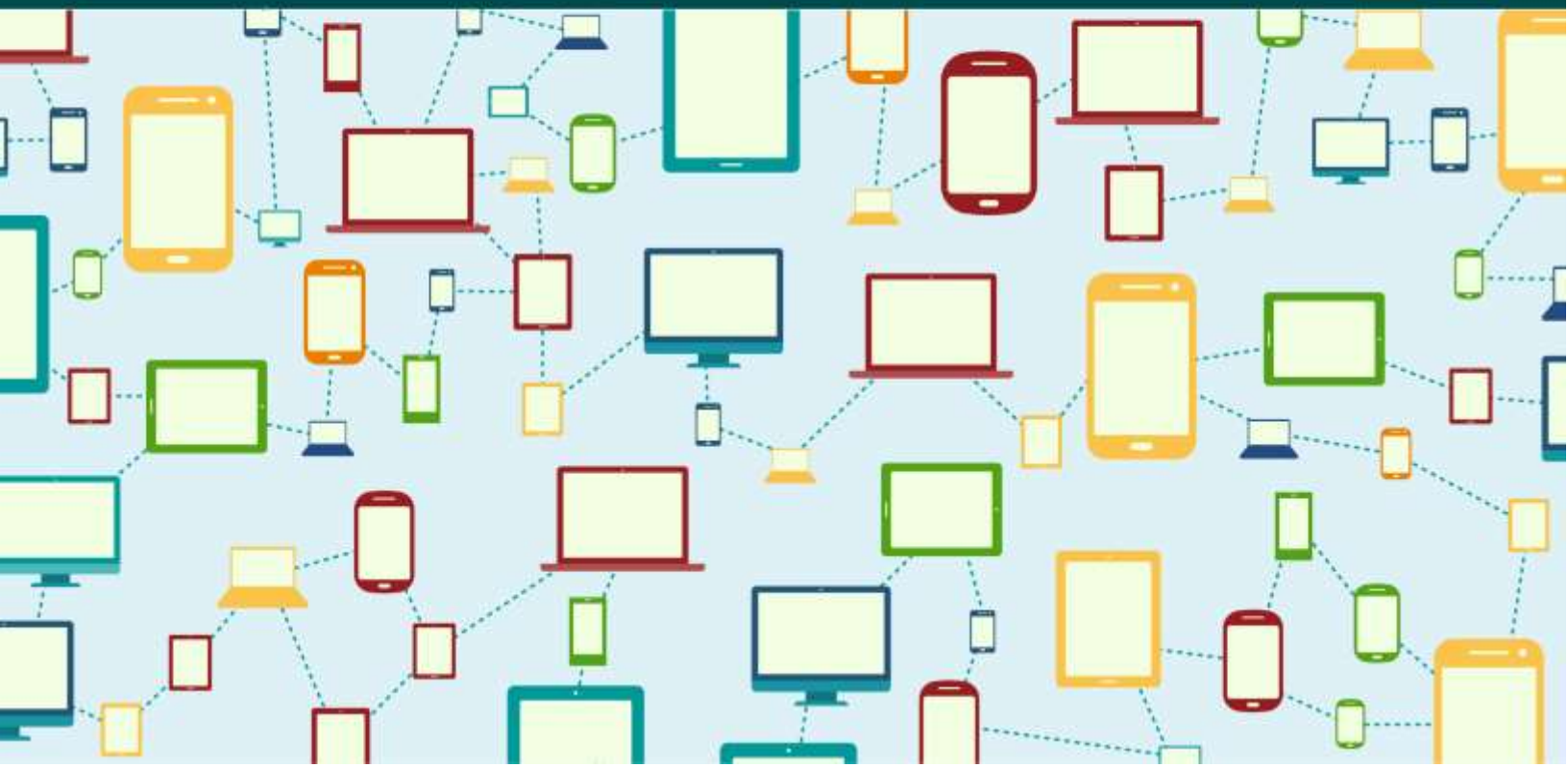
fido ALLIANCE | simpler stronger authentication



FAQ on FIDO Relevance for the GDPR

September 2018

General Data Protection Regulation

Full copy of regulation: https://gdpr-info.eu/

Audience

This document provides answers to questions on authentication, user consent, use of biometrics…in the context of the European Union (EU) General Data Protection Regulation (GDPR). It shows how FIDO authentication can help service providers comply with the regulation.

Introduction

After four years of preparation and debate, the EU GDPR was approved by the EU Parliament on 14 April 2016. Enforcement began on 25 May 2018 - at which time organizations had to be compliant.

Strong authentication based on FIDO Alliance protocols help maintain the privacy of end-users and secure access to data. They were developed with a "privacy by design" approach and align with tenets of the GDPR.

The GDPR is a data privacy regulation that mandates companies implement safeguards to protect the data they collect and store. GDPR replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' rights to data privacy, and to reshape the way organizations across the region approach data privacy.

Who falls under the GDPR directive?

The GDPR applies to all organizations processing and holding the personal data of subjects residing in the European Union, regardless of the organization's physical location.

How do companies achieve GDPR compliance?

One of the key components for GDPR compliance is the need to control access and permissions on data. The European Union Agency for Network and Information Security – ENISA – describes authentication as 'key to securing computer systems' (Privacy And Data Protection By Design, Section 4.1.1) and as the first step 'in using a remote service or facility, and performing access control'. Referenced in the description as GDPR-compliant authentication solutions are one-time password solutions (push), smart cards, and FIDO protocols. Many online authentication and identity technologies store user data and cryptographic secrets in centralized servers. An essential feature of FIDO is that it does not store any means of personally identifiable information (PII). Also, FIDO does this without sharing any information between online services. These privacy measures help make FIDO an option for GDPR compliance.

What specific GDPR categories can benefit from FIDO strong authentication?

Data security (GDPR Article 5, 32), consent and individual rights (Article 7, 16-20), and biometrics (Article 4, 9, Recital 91). Read the full GDPR white paper. In general, however, strong multifactor authentication, is a fundamental part of cybersecurity and data protection. Given the prevalence of breaches over the past few years, and that 81% of them exploited stolen credentials, multifactor authentication is a critical ingredient in any data protection program.

Will passwords be outlawed by the GDPR?

No. The GDPR mentions appropriate security controls, not specific guidance. A password that satisfies a company's risk assessment is acceptable under the GDPR. That could include air-gapped machines run in a physically secure environment. The GDPR, under article 32-1, says "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…" However, for sensitive personal data, such as healthcare data or other data described in Article 9 of the regulation, strong authentication may be necessary to protect access.

Where is strong authentication specified in the GDPR's articles?

There are no specific mentions of authentication contained in the main body (Articles) of the GDPR document. The word "authentication" does appear twice in the Recital sections, which are used to determine what any directive or regulation means in the context of a particular court case. There are, however, compliance regulations that describe requirements that may be addressed with FIDO protocols, namely strong authentication, data privacy, consent, and biometrics.

Is biometric or two-factor authentication the bulk of what I need for GDPR compliance?

No. The GDPR is a legal privacy framework that sets guidelines for the collection and processing of personal information of bonafide citizens and/or residents of the European Union (EU). This framework covers any company, regardless of physical location. Meeting GDPR compliance means companies will need policies, processes, and tools to facilitate compliance. One piece of the puzzle can include FIDO Alliance protocols for strong authentication, which call for strict privacy protections.

How does the GDPR view biometric authentication?

Biometric data is viewed broadly, and in many cases requires privacy impact assessments for its processing. The GDPR puts biometric data in the "sensitive" category for personal data. This means it warrants robust protection and restrictions on its use. FIDO Alliance standards prohibit biometric data from being stored or matched on servers as a result, the biometric data never leaves the user's device. This characteristic is a key privacy aspect within FIDO protocols. The GDPR allows Member States to pursue divergent protections for biometric data. For example, CNIL (France's Data Protection Authority - DPA) has put out rules requiring that CNIL review and authorize applications where biometric templates are matched on remote servers – but waiving the need for CNIL authorization for applications that "match on device" and meet several key criteria, much of which aligns with FIDO Alliance protocol design.

User consent is an important construct for FIDO, what does the GDPR say about consent?

Recital 42 and Articles 6 and 7 of the GDPR says the controller of data should be able to demonstrate that the owner of the data has given consent to process that data. Article 6 says processing is only lawful if the user has given consent, and the company processing the data must be able to show the user consented. Recital 51 and Article 9 calls for explicit consent for sensitive data, although both terms are open to interpretation. Both requirements are addressed by the requirement for "user presence" at the computer executing multi-factor authentication and a digital "signature" as a means to providing and proving consent.

Data processors need 'explicit' or 'unambiguous' data subject consent - what is the difference?

The conditions for consent have been strengthened to eliminate long illegible legal terms and conditions. Request for consent must be given in an intelligible and easily accessible form, with the reason for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear and distinguishable from other matters, using clear and plain language. Explicit consent is required only for processing sensitive personal data - in this context, nothing short of “opt in” will suffice. FIDO protocols provide both user consent mechanisms and digital signature capabilities.

What other foundational elements of FIDO are important for GDPR compliance?

The fact that FIDO authenticators execute user verification locally and that they do not share keys are important security constructs that align with Recital 78 and 108 of the GDPR, which states that companies should adopt policies and measures that meet the principles of data protection by design. Furthermore, Article 25-1 states companies should implement appropriate measures that are designed to implement data-protection principles. FIDO protocols meet these requirements.

What are the penalties for non-compliance?

Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 million, whichever is greatest. Fines are 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. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

What constitutes personal data?

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

What is the difference between a data processor and a data controller?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

Contributors

Tommaso De Orchi, Yubico

John Fontana, Yubico

Jeremy Grant, Venable

Alain Martin, Gemalto

Arshad Noor, StrongKey

Andrew Shikiar, FIDO Alliance