# HOW WICKR CAN HELP YOUR ORGANIZATION BECOME COMPLIANT WITH GDPR

wickr

## What is GDPR?

The General Data Protection Regulation, or **GDPR**, presents a sweeping set of regulations defining how businesses process and protect the data of EU consumers. The policy upgrade is mainly driven by the urgency to modernize the protections to fit today's global interconnected realities and to provide safeguards to the EU consumers served by foreign businesses, often regulated by weaker privacy laws.

## Why does GDPR matter to my business?

Under GDPR, any organization processing the personal and sensitive data of EU citizens is responsible for ensuring much higher standards for safeguarding the information, regardless of the business' location.

Starting May 2018, businesses that are found in non-compliance with GDPR will face steep penalties, including fines of up to 4% of global revenue.

Even if your organization may not be directly covered by GDPR, your customers or partners may be, which makes it important for your organization to boost your GDPR readiness in time for May 2018.

In addition, demonstrating a higher commitment to user privacy and transparency is always a good business practice which helps to build trust among your customers.

# What is changing under GDPR?

In its **99 articles**, GDPR promotes significantly higher information security standards, namely encryption, access control and data minimization. It also empowers consumers to have control and easier access to their data, a comprehensive penalties regime, and a clear responsibility for organizations to obtain user consent before collecting information about them.

Specifically, under GDPR, businesses are encouraged to adopt the data protection by design and by default approach to managing personal and sensitive information, which includes:

- End-to-end security throughout data's lifecycle to ensure all personal information is securely processed and destroyed when no longer needed;
- Data encryption as an appropriate technical measure to ensure that, by default, personal data is not accessible to unauthorized persons;
- Data minimization to ensure that, by default, only necessary personal data is processed or collected and only for the necessary period of time;
- Accountability and transparency in processing personal and sensitive data: under GDPR, businesses must clearly describe data collection, processing, and security measures taken to protect consumer data;
- Breach notifications requirement under GDPR applies to any business: companies have to report data breaches within 72 hours to both data regulators and affected consumers unless encryption was applied to breached data, rendering it effectively unintelligible to any person who is not authorized to access it.

**More on the changes to the EU data protection regime >>**

# Preparing for GDPR Compliance

While many US and international companies have started on the path to getting ready for GDPR, many still **remain** in the assessment phase of identifying the risks and data security gaps. A large number of businesses see information security enhancement as a top priority in getting to the GDPR compliance.

According to the **GDPR Preparedness Pulse Survey** by PWC, “77% of companies plan to allocate $1 million or more on GDPR readiness and compliance efforts, with 68% saying they will invest between $1—$10 million and 9% expecting to spend over $10 million to address GDPR obligations."

Collaboration among distributed teams and with international partners is key to your business growth. However, it may also create risks for data protection which, under GDPR, you are required to assess and minimize. Protecting your organization’s business communications through Wickr Pro can make your collaboration easy and compliant with GDPR.

# Private by design and by default

When you launch your own private communications network on Wickr Pro, you are in full control of any and all valuable information. Wickr never has access to your communications, serving de facto as a secure black box for your business content. Your conversations and files do not touch Wickr servers unencrypted and aren't stored server-side. When audited for compliance, your secure collaboration service should fall out of the audit scope, making the process easier for your organization.

# End-to-end security

All applicable security measures outlined in GDPR are built into Wickr's secure collaboration platform:

**Encryption in transit and at rest**

Wickr's multilayered end-to-end encryption ensures the highest possible level of protection for all business communications that contain personal data (PHI/PII), rendering it inaccessible to anyone beyond authorized parties. This enables your company to invoke an exception to notifying users of a breach of such encrypted information. With Wickr, privacy is not just a promise, it is mathematically ensured.

**Ability to ensure the ongoing confidentiality and integrity of data**

Wickr enables your employees to verify and maintain the confidentiality and integrity of communications through the easy-to-use cryptographic key verification process within the platform.

**Regular testing, assessment of the effectiveness of technical and organizational measures for ensuring the security of data**

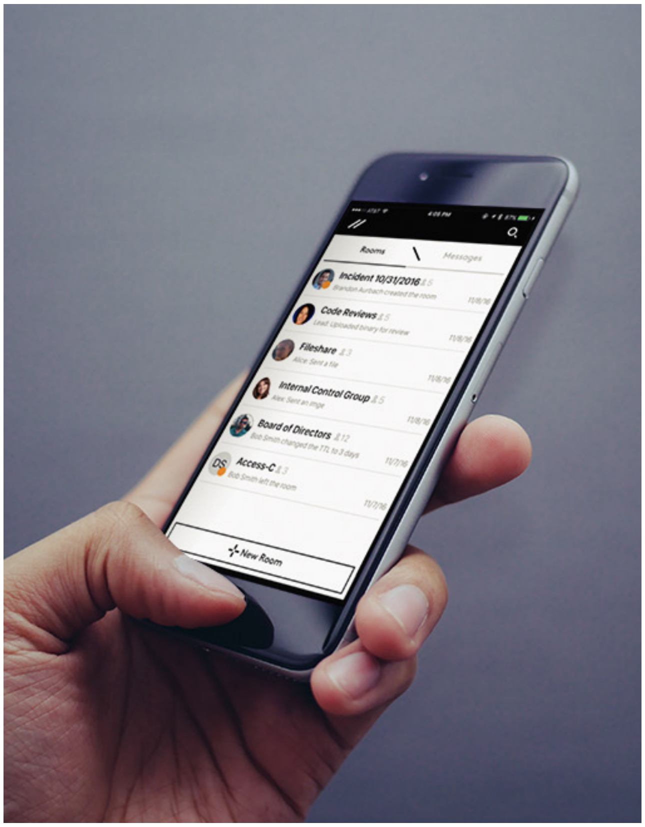
To validate our privacy and security assurances, Wickr undergoes the internal security testing in addition to engaging independent security teams and the open source community in auditing our source code.

**Learn more about Wickr Security>>**

## Data minimization:
In the cloud or in your own hosted environment

Wickr Pro does not record, collect, or retain any personal or sensitive information beyond what is necessary to provide service. In addition, all your business communications are ephemeral by design and by default to ensure that valuable communications content is only accessible for the necessary period of time and is destroyed when no longer needed. For these reasons, companies deploy Wickr's secure transport layer to enable reliable and private data transmission protecting support operations, deal workflow, payment processing, device-to-device communications (IoT), and other business transactions.

Wickr’s global server infrastructure is designed to accommodate your GDPR compliance needs.



## Accountability and transparency

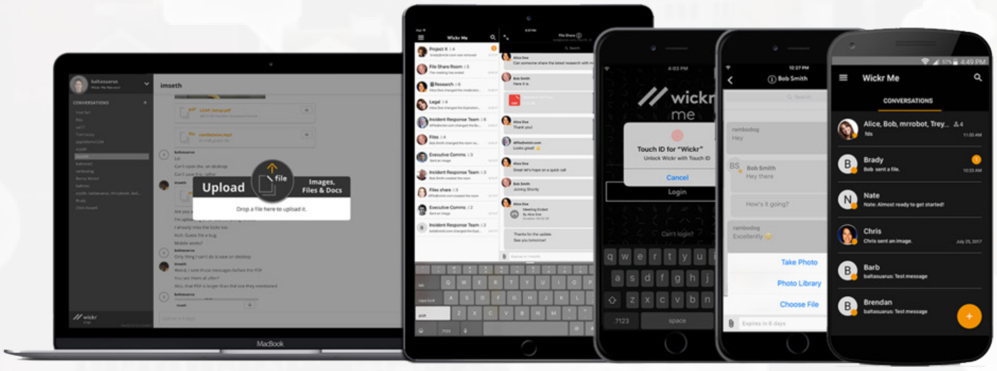
When shared via Wickr secure channels both internally or externally, your sensitive business data, including personal consumer information, is protected end to end and controlled by you. Through the Wickr Network Dashboard, you can manage security, policy, and compliance across your entire organization.

# How is Wickr preparing for GDPR?

From its launch in 2012, Wickr has built all of its communications solutions private by design to empower our users to take complete control over their private communications – from beginning to end. As a team of security experts and privacy advocates, we have always believed that the most reliable path to protecting your personal and sensitive data from security compromise is to never have access to such content transmitted through Wickr networks and to ensure that data which is no longer needed is simply not retained. In recognition of our commitment to protecting user privacy and our transparency practices, Wickr has been repeatedly **awarded** an all-star rating by the Electronic Frontier Foundation.

**Learn more about Wickr's privacy commitment >>**

As you transform your data protection practices to fit the GDPR compliance requirements, consider Wickr Pro as part of your core GDPR solution. Switching your most important business communications to an end-to-end encrypted and ephemeral network makes your transition to GDPR-friendly operations easy and cost-effective.



**TRY WICKR PRO ►**

**www.wickr.com | sales@wickr.com**