Are you GDPR-compliant?

Preparation is costly. So are the fines. The good news is that KSI solutions support GDPR compliance.

GDPR Background

The General Data Protection Regulation (GDPR), enacted in 2018, is a data protection law that sets forth a uniform standard for processing and storing the personal data of EU citizenry. The most sweeping privacy regulation to impact the global marketplace in decades, GDPR was created by the European Parliament, Council of the European Union, and the European Commission. Among other things, GDPR establishes criteria-based penalties for organizations not in compliance with its directives. Adherence to the new law is mandatory.

GDPR is a government-led effort to protect the personal data of EU citizens

▼

GDPR sets standards for compliance

▼

GDPR establishes penalties for non-compliance

GDPR impacts companies around the globe, not just those located in the EU

The maximum fine levied by the GDPR is 4% of global turnover, or €20 million, whichever is greater.

One year post-enactment, with 90,000 breaches so far reported and 100+ penalties imposed, the world's 500 largest corporations are on track to spend a total of $7.8 billion on compliance.

GDPR is extraterritorial, impacting not only companies located in the EU, but also those residing outside its borders.

GDPR applies to all organizations holding and/or processing the personal data of citizens residing in the EU, no matter their physical location.

How is GDPR enforced?

Independent, public oversight authorities have been established in each EU country to monitor and enforce application of GDPR, address noncompliance, highlight data controller and processor obligations, and promote awareness of privacy rights and risks. While media reports have focused on imposition of the largest fines, enforcement has varied widely by country, with penalties levied against companies large and small for a variety of infractions.

How does KSI support GDPR compliance?

KSI peripherals control access to private data with use of multifactor authentication for logon and in-app reauthentication. Fingerprint biometrics and proximity-based RFID – integrated as optional security components within KSI keyboards and authentication pods – support GDPR compliance by identifying and allowing only authorized users to enter areas where private data is stored. Our security products eliminate the need for passwords that can be stolen or otherwise compromised to gain access to private data. KSI peripherals support Privacy by Design principles emphasized by GDPR as being a critical factor in information system planning and the prevention of invasive events before they occur. KSI products complement your overall GDPR strategy.

What are your responsibilities under GDPR?

Selected, summarized excerpts from GDPR

Article 5

GDPR directs that data be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Article 24

GDPR states the controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the regulation and that the measures will be reviewed and updated where necessary.

Article 32

GDPR states that data controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and ensure the ongoing confidentiality and integrity of processing systems. GDPR requires data processors and controllers to consider the risk associated with data processing, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

Recital 49

GDPR warns that companies need to be concerned about the ability of a network or information system to resist, at all levels, accidental events or unlawful or malicious actions that compromise stored or transmitted personal data. Going further, Recital 49 states this could, for example, include preventing unauthorized access to electronic communications networks, malicious code distribution, and damage to computer and electronic communication systems.

This document is presented for informational purposes only and in no way constitutes legal advice. Consult with legal counsel in planning and adopting your GDPR strategy.
Visit https://eugdpr.org/ to gain a deeper understanding of GDPR and its provisions.