PRESCIENT SECURITY

Guard with **GDPR**

In 2018, the EU enacted the General Data Protection Regulation (GDPR) in response to growing concerns over the protection of personal data for EU citizens. The regulation requires businesses to protect individual's personal data, such as email addresses, IP addresses, and location, and respect fundamental data privacy rights.

If you've ever gone online while in Europe, you may have noticed how frequently sites ask for consent regarding data and cookies. Consent is a major factor of GDPR. Organizations must ask to collect people's data in a specific, clear manner and give them a say in what happens with it. If there's a breach in data privacy, businesses are required to notify the authorities and in some cases the individuals themselves. Failure to meet any of the regulations can result in fines and restrictions from the EU.

Who Needs GDPR?

Any organization that handles personal data for those living in the EU or EEA is required by law to comply with the GDPR. The regulations have international reach, which means that even if a company isn't based in the EU, they're still subject to its rulings. It affects everything from international online retailers to third-party data processors such as Google Drive.

Examples include

Any entity that handles EU personal data, such as:

- ✓ Businesses
- ✓ Non-Profits
- ✓ Public-Authorities

The Core Principles of GDPR:

Lawfulness, Fairness, and Transparency

Data processing must be **lawful, fair,** and **transparent** to the person whose data it is – this is usually communicated in GDPR documents as the "**data subject**".

Purpose Limitation

Anyone processing personal data must do so for **legitimate purposes** that are **clearly communicated** when that data is collected.

Data Minimization

Only data that is **completely necessary** should be collected and processed.

Accuracy

Personal data has to be **accurate** and updated frequently to remain as such.

Storage Limitation

Personal identifying data **can't be kept in perpetuity** just for the sake of it. It can only be stored while it's needed for the purpose stated from the start.

Integrity and Confidentiality

Data processing must be **secure** and handled with **integrity** and **confidentiality**.

Accountability

When it comes to accountability, the **data controller is responsible for demonstrating compliance** with the aforementioned.

The Benefits and Competitive Advantages of GDPR

Demonstrated Commitment to Customer Protection and Data Governance: A designation provided Fundamental to GDPR compliance is developing strong data management frameworks. These include risk management strategies, clear lines of accountability, and constant data security monitoring. This builds proper data governance, which ensures that businesses and their customers are better protected.

Reduced Risk of Breaches and Fines: A ripple effect of better data governance is that organizations are better protected against breaches and the associated reputational damage and expensive fines.

Better Data Management: GDPR is a useful and practical guide on how data can be managed more securely.

A Competitive Advantage in the Global Marketplace: The adoption of GDPR ensures that businesses are primed to engage with the more than 400 million people residing in the EU.

Boosts Customer Trust: It's not just tech insiders that care about data privacy anymore. Showing compliance with the GDPR is a way to signal to those who care about privacy that they can trust your organization.

You're Prepared for the Future: Though limited to the EU right now, governments around the world are increasing their data regulations and largely using the GDPR as a baseline. Getting GDPR compliant now, even if organizations aren't operating in the EU, means that as new regulations get rolled out orginzations already have the necessary frameworks in place and aren't forced to do massive overhauls.

Prescient Security and GDPR

Through Data Protection Impact Assessments, GDPR Gap Analysis and Strategy Development, Policy Development and Staff Training, Data Processing Records Management, and Breach Response and Notification Management, Prescient Security provides a structured approach to GDPR Compliance. Our team at Prescient Security is ready to assist with all your GDPR needs and answer any questions you may have.

A Global Top 20 Independent Audit and Penetration Testing Company, Prescient Security delivers unparalleled quality in audits, attestations, and certifications to ensure excellence and client success. Using a Risk-Based Audit Approach versus a Requirement-Based Audit Approach, paired with the ability to customize audit deliverables based on specific client needs, Prescient Security operates from a cybersecurity standpoint first, is comprehensive yet granular, and in a fraction of the time.