SecurityMetrics

Guide to GDPR Compliance

GDPR Solutions for Small to Medium-Sized Businesses

securityMETRICS®

Guided GDPR Overview

SecurityMetrics GDPR Defense is a tool that keeps your GDPR efforts organized and progressing.

With GDPR Defense, you can access a guided checklist of requirements so you aren't left wondering what's required of you.

You can also upload your GDPR policies to a central storage cloud, access your GDPR implementation report, easily implement GDPR policies using our convenient templates, and train your workforce—all GDPR best practices.

Finally, you can gain peace of mind knowing that if you are storing unencrypted sensitive data, you can quickly discover it using our PIIscan tool.

Take the pain out of complying with GDPR requirements with SecurityMetrics GDPR Defense.

1 Learn the Requirements

Don't be left wondering what's required of you

2 Implement GDPR Best Practices

Meet requirements and close gaps in your security environment

3 Secure Your Data

Discover data and reduce liability

1 2 3

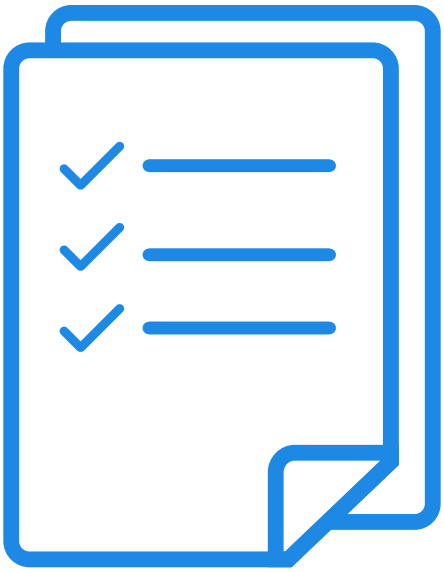
Learn the Requirements

ASSESS YOUR COMPLIANCE WITH A GUIDED CHECKLIST

Track your compliance progress simply and quickly with SecurityMetrics' guided GDPR checklist. Our checklist breaks down important elements of the GDPR into actionable items so you aren't left wondering what you need to do next. It also monitors your progress in real time and features an organized dashboard for straight-forward reporting.

The checklist covers:

- Privacy Policy and Processes
- PII Data Mapping and Tracking
- Individuals' Data Rights
- Data Breach Processes
- Data Retention and Protection by Design and Default



Implement GDPR Best Practices

UPLOAD GDPR POLICIES TO A CENTRAL LOCATION

An additional feature of the SecurityMetrics GDPR checklist is the ability to store your policies in a central storage cloud, which makes them easily accessible if you need to provide proof of implementation. Feel at ease knowing that your policies are stored securely in the event of a hard drive crash or data loss.

STAY ON TOP OF YOUR PROGRESS WITH REAL-TIME REPORTING

In the event of a data breach, you can use the SecurityMetrics GDPR Implementation Report as proof of your efforts. The report is easily accessible from our checklist dashboard and provides a pie graph of your implementation progress, as well as a report of your progress over time.

TRAIN YOUR WORKFORCE

Keep your employees up to speed on GDPR best practices with the GDPR Fundamentals training course, an interactive experience that is both informative and memorable. At the conclusion of the course, there is an assessment to validate learning.

IMPLEMENT GDPR POLICIES AND PROCEDURES

Part of the GDPR requires businesses to update and expand their policies and procedures to meet new regulations, such as data subject rights, consent, data retention, and breach notification. Rather than trying to build your own GDPR Policies & Procedures from the ground up, we provide templates that you can easily tailor to fit your business.

Secure Your Data

FIND PII AT YOUR ORGANIZATION

SecurityMetrics PIIscan is a data discovery tool that assists with GDPR requirements by discovering unencrypted Personally Identifiable Information (PII). PIIscan searches computer systems, hard drives, and attached storage devices for unencrypted PII. Once PIIscan has discovered unencrypted PII, a report is generated that displays where the data is located. This makes it easy to securely delete or encrypt discovered data, reducing your organization's risk. By using PIIscan, you will also save time by not needing to manually search for unencrypted PII on your systems.

"[GDPR Defense] was simple and easy and not expensive for my company. With the help of SecurityMetrics we completed it with no hassle. Thank you [for the] technical help."

-RICHARD STUDT

Director, Pwllheli Amusements Ltd.

GDPR Defense US Pricing

BASIC	PLUS
$199.99	$699.99
GDPR Defense Checklist	GDPR Defense Checklist
Policies Storage Cloud	Policies Storage Cloud
Real-Time Reporting	Real-Time Reporting
PIIScan	PIIScan
Workforce Training*	Workforce Training*
	GDPR Policy & Procedure Templates*

*Available for individual purchase.

GDPR Defense UK Pricing

BASIC	PLUS
£147.99	£536.00
GDPR Defense Checklist	GDPR Defense Checklist
Policies Storage Cloud	Policies Storage Cloud
Real-Time Reporting	Real-Time Reporting
PIIScan	PIIScan
Workforce Training*	Workforce Training*
	GDPR Policy & Procedure Templates*

*Available for individual purchase.

Price varies based on conversion rate.
All SecurityMetrics GDPR Compliance packages are an annual subscription that will be automatically renewed.

GDPR Compliance FAQ

WHAT IS GDPR?

GDPR stands for General Data Protection Regulation. It was designed to harmonize data privacy laws across Europe, protect and empower all EU citizens with data privacy, and to reshape the way organizations across the region approach data privacy. This mandate replaces the 1995 EU Data Protection Directive and was finally approved by EU parliament on April 14, 2016 after four years of preparation and debate. It went into effect 20 days after its publication in the EU Official Journal—in May of 2016—and has been applicable in all member states since May 25, 2018.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Organizations can be fined up to 4% of annual global turnover (aka revenue) or €20 Million—whichever is greater—for violation of GDPR. These are the maximum fines that can be imposed for the most serious infringements, like insufficient customer consent to process data or violation of the core "Privacy by Design" concepts.

According to article 28, there is a tiered approach to fines. A company can be fined 2% of annual global turnover for not having their records in order, not notifying the supervising authority and data subject about a breach, or not conducting an impact assessment.

It is important to note that these fines apply to both controllers and processors, and data 'clouds' will not be exempt from GDPR enforcement.

WHO DOES THE GDPR AFFECT?

The GDPR applies to any organization that handles the personally identifiable information (PII) of EU citizens, whether that organization is in North America, Europe, or somewhere else in the world.

PII is data kept by an organization which can be used to "distinguish or trace an individual's identity." PII could include names, birth dates, birth places, mothers' maiden names, addresses, emails, IP addresses, or social security/ insurance numbers, such as UK National Insurance Numbers (NINO). "Linked PII" is any information that is linkable to an individual, like educational, medical, employment, or financial information. PII also includes payment card details such as the magnetic card stripe (also known as track data) and primary account numbers (PAN).

You also need to know what type of organization you are considered under GDPR compliance, since your GDPR responsibilities might vary slightly based on whether you're a data controller or processor:

- **Data Controller:** Entities or individuals that need to process personal data in order to do business. They determine the purposes for which and the manner in which the personal data is processed.
- **Data Processor:** Processors take and/or process personal data on behalf of the Controller.

GDPR COMPLIANCE REQUIREMENTS OVERVIEW

Here are a few key GDPR requirements you should know about:

- **Breach notification:** Data controllers must report personal data breaches no later than 72 hours after they are aware of the breach.
- **Consent:** Consent must be obtained from individuals for processing personal data.
- **Data Protection Officers (DPO):** Appointing DPOs will be mandatory for companies that are public authorities, process high volumes of personal data, or process special categories of personal data.
- **Data subject access requests (DSAR):** The time limit to comply with DSAR has been reduced from 40 days to one month.
- **Privacy by design:** Products, systems, and processes must consider privacy-by-design concepts during development.
- **Privacy Impact Assessments (PIA):** PIAs must be carried out in certain situations.
- **Privacy notices:** Privacy notices must be more transparent, using clear and plain language, and easily accessible.
- **Profiling:** An individual has the right to not be subject to profiling, and profiling for marketing purposes will always require explicit consent.
- **Record keeping:** Each data controller must keep a record of processing activities.
- **Right to portability:** Users may request a copy of personal data in a portable format.
- **Right to erasure:** Data subjects have the right to request for their data to be deleted.
- **Right to object:** Individuals should be advised that they have the right to opt out of direct marketing.

Some aspects of the GDPR are easier to interpret than others. For example, the GDPR says that data owners are required to have an opt-in choice presented to them before a company can begin storing, processing, or transmitting their personal information. It's easy to determine whether that requirement has been met or not.

On the other hand, the GDPR states, "protect your data by design and default." With this requirement, it's difficult to know if you're perfectly compliant because it eludes to a lot of data security practices.

Even though GDPR compliance isn't currently as well-defined as a standard like the Payment Card Industry Data Security Standard (PCI DSS), it's important to be aware of and implement reasonable data security best practices. It's impossible to say with absolute clarity that an entity is absolutely compliant with GDPR because associated testing procedures are not specifically defined yet. Currently, various supervisory authorities are working on checklists and similar guidance, which indicates that there will likely be more specific audit protocols as time goes on.

For the time being, you can actively and carefully address GDPR regulations, document your efforts, collect your results, and show risk analysis/ assessment results.

One of GDPR's primary purposes is to help organizations protect individual's data, ensuring that organizations improve their data security.

To Discuss Your Business's GDPR Needs, Contact Us.

801.995.5656
compliance@securitymetrics.com

securityMETRICS®