Netsurion®

Powering Secure and Agile Networks

# GDPR Compliance Guide

## How Netsurion® Can Help You Achieve and Maintain Compliance

## Summary of GDPR

The European Union General Data Protection Regulation (GDPR) (Regulation 2016/679, Apr. 27, 2016), approved by the European Parliament and the Council of the European Union, replaced the Data Protection Directive (Directive 95/46/EC) effective May 25, 2018. GDPR provides requirements for companies that use or process data in the European Union (EU), or simply use or process data about EU citizens anywhere in the world. The reforms give European consumers new rights and control over their personal information, and impose new obligations on businesses to the extent that they collect personal information from EU citizens, regardless of where they reside, or individuals who reside in the EU, regardless of their nationality.

The GDPR rules empower individuals by, among other things:

- Providing easier access to personal data and more information on how data is processed
- Facilitating data portability, or transfers of personal data between service providers
- Clarifying the fundamental "right to be forgotten" for individuals who no longer wish for their data to be processed, and
- Requiring expedited notifications to the national supervisory authority by companies that experience a data breach affecting personal data

While some of the measures serve to make the system less cumbersome, the broad reach, advanced restrictions, expanded obligations and enhanced penalties imposed on businesses could more than offset these reductions. The task of mapping data flows, creating relevant compliance structures, and developing internal data and IT processes takes planning. Given the magnitude of GDPR requirements and potential fines, it will be important for companies to maintain compliance over time. Fines and penalties to date have totaled $150 million USD (£ 114 million).

Developments like Brexit – the withdrawal or exit of the United Kingdom from the EU – also impact data privacy and protection regulations over time. In other cases, European countries have been slow to enact local laws in accordance with GDPR that limit enforcement and the number of people in the EU who can file a complaint. In addition, following widespread and ongoing data breaches, several countries globally have enacted their own version of data protection regulations inspired by GDPR.

## Simplify GDPR Requirements and Compliance

### Personal Data

The term "personal data" means "any information concerning an identified or identifiable natural person". An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. The Regulation does not apply to personal data rendered anonymous so that the data subject is not identifiable.

### Extraterritorial Effect

The Regulation applies to not only the processing of personal data by controllers who are in the EU by a controller or a processor not established in the EU, if the processing activities are related to offering goods or services to the data subjects or monitoring their behavior within the EU.

### Lawfulness of Processing

To be lawful, at least one of the following must apply :

The data subject consents:

- Processing is necessary for the performance of a contract to which the data subject is a party;

- Processing is necessary for compliance with a legal obligation to which the controller is subject (under EU or Member State law);
- Processing is necessary to protect the vital interests of the data subject or another natural person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (under EU or Member State law);
- Processing is necessary for legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### Consent

Consent to processing must be unambiguous, specific, informed, and freely given (e g., checking a box at a website or choosing technical settings). Pre-checked boxes do not constitute consent. For sensitive data (e.g., data revealing race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation), consent must be explicit. When processing has multiple purposes, consent should be given for all of them. Consent may be withdrawn.

### Data Processing

The processing of personal data must be lawful, fair, and transparent. Individuals should be made aware of the risks, rules, safeguards and their rights in relation to the processing of personal data. The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection. Personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Time limits should be established for erasure or periodic review. Personal data should be processed in a manner that ensures appropriate security and confidentiality.

### Right to Be Forgotten

Individuals have a right to request deletion of data, with some exceptions (e g., if retention is legally required).

### Data Portability

Individuals have the right to transfer personal data between different service providers, with ease.

### Children

Special rules apply to children's data. When a child is below age 16, processing is lawful only if parents or guardians consent. Member States may establish that a "child" is younger than age 16 for these purposes, so long as the age is not below age 13.

### Controller Responsibility

Personal data must be processed under the responsibility and liability of the controller, who must ensure and document compliance for each processing operation. Controllers should only use processors who provide sufficient guarantees in terms of expert knowledge, reliability and resources to implement technical and organizational measures that will meet the requirements of the Regulation. Adherence to an approved code of conduct or certification mechanism maybe used to demonstrate compliance. There must be controller-processor agreements in place that describe the subject matter, duration, nature and purposes of the processing, type of personal data, and categories of data subjects. Upon completion of the processing, the processor must, at the controller's election, return or delete the data, unless the processor required by law to store it. Joint and several liability for controllers and processors.

### Privacy Impact Assessments

Data controllers must conduct Privacy Impact Assessments (PIAs) for "risky" processing. If PIA indicates that processing involves a high non-mitigatable risk, controller should consult supervisory authority prior to the processing.

### Data Protection Officer

Organizations with 250 or more employees must appoint a Data Protection Officer (DPO) to be tasked with informing controller/processor and employees about their obligations with regard to processing, monitoring compliance with the Regulation, employee training, and audits; providing advice regarding PIA; cooperating with the DPA; and serving as contact point for DPA on issues relating to processing. The DPO must function independently in performing these tasks.

### Documentation

Controllers and processors must document all processing and make documentation available to DPA on request.

### Data Breach Notification

Controllers must notify DPA within 72 hours of learning of a breach, where feasible; no notification is required if a breach is unlikely to result in risk to the rights or freedoms of individuals. Controllers must notify data subjects without undue delay, where the breach is likely to result in a high risk to their rights or freedoms. Notifications to data subjects should describe the nature of the breach and recommendations for individuals to mitigate potential adverse effects. Processors must notify controllers.

### Streamlined Approvals

A single DPA can be designated the lead, enabling multiple DPAs to handle cases in a more streamlined manner.

### Codes of Conduct and Certification

Codes of conduct are encouraged, and are subject to approval by the Commission and an appropriate expert, accredited body, should monitor compliance. Approved codes of conduct will be registered and published. Data protection certification, seals and marks are encouraged.

### Transfers to Other Countries

Transfers to other countries are permitted based on a determination that the country provides adequate protection of privacy; transfers are subject to adequate safeguards (e.g., binding corporate rules, standard contractual clauses, an approved code of conduct, approved certification mechanisms, explicit informed consent (limited), etc.).

### Reduced Notifications

Supervisory notifications about data processing are no longer required, but permission is required to process certain categories of data.

### Article 29 Committee

Article 29 Committee will be "upgraded" to an independent European Data Protection Board.

### DPA Enforcement

Data Processing Agreements (DPAs) have enhanced enforcement powers, including expanded investigatory authority.

### Complaints and Remedies

EU citizens can lodge complaints with local DPAs, even where data is processed extra-territorially, and have the right to a judicial remedy against supervisory authorities who fail to act and against controllers and processors.

### Penalties

DPAs are authorized to impose fines of up to 4% of global annual turnover for certain serious infringements or 2% for less serious infringements.

## Maximize GDRP Readiness

Netsurion can help your organization meet the requirements of the GDPR.

Data classification is the foundation of any successful information GRC (Governance, Risk and Compliance) initiative. It limits corporate liability and reduces the risk of data leakage, while increasing the productivity and competency of users.

Netsurion can help organizations meet the GDPR requirements by alerting when sensitive data is accessed and by enforcing access and usage rights on PII (Personally Identifiable Information) whether it is at rest, in transit, received, handled, or shared. Additionally, EventTracker delivers comprehensive audit trails that enable forensic data analysis, so that your organization can know "who" did "what", "when", and "how" with the data.

## The Challenges of the EU GDPR

Here are challenges organizations are faced with regarding the GDPR, and how the EventTracker platform can help your enterprise gain and maintain compliance.

### Focus on Personal Data: The right to be forgotten

The GDPR defines personal data rigorously, referring to any information that could be used, on its own or in conjunction with other data, to identify an individual.

EU citizens will have to explicitly agree with the storage, use, and management of their personal data, and will still have the right to access, amend, or request its deletion. Plus, they will be able to oppose certain types of processing, such as profiling for marketing purposes.

Netsurion can help by:

- Allowing Personally Identifiable Information (PII) to be automatically alerted, whenever it is received, handled, or shared in the form of an unstructured file (e.g. an email, Word or PDF document, Excel spreadsheet, PowerPoint presentation).
- Providing a content, context and metadata aware policy engine that identifies PII, alerts on user actions to classify the file according to policy, applies protective markings and labels to identify the information and decrease corporate liability.

### Mandatory Data Breach Notification and Information Governance

Organizations are required to actively track how and where data is stored and used through the supply chain. This means adopting risk management tools and building security and privacy into your operations by design. Also, the GDPR requires organizations to report data breaches to the regulators and the individuals whose data was breached, within 72 hours. The data breach and the security measures present at the time of breach will be evaluated by the supervising authority to determine the fine to be levied and to ensure future compliance.

Netsurion can help by:

- Delivering a comprehensive audit trail that documents and traces any authorized and unauthorized access to confidential data.
- Enabling enterprises to leverage EventTracker to correlate events and generate dashboards, alarms and reports, knowing in real-time who is doing what, when, and how with classified information.
- Detecting and alerting on sensitive data to help identify information requiring special handling, allowing for easily adding extra descriptors, customized tooltip texts for each classification, or custom-configured text labels for each security classification.

**Joint Accountability**

The GDPR defines data controllers as individuals or organizations who determine the processing of EU citizens' personal data, and data processors as those who may manage, modify, store, or analyze that data on behalf of or in conjunction with the controllers (like cloud providers and outsourcing firms).

According to the GDPR, both parties will now be jointly responsible for complying with the new rules. This means that if an organization outsources data entry or analysis to a third party, or processes data on behalf of another organization, they will both be liable.

We can help by:

- Alerting users when sensitive data is leaving the organization to warn or prevent them from sending data outside of the organization.
- Delivering a way to control access to sensitive information across a myriad of third parties. EventTracker SIEM applies protection to e-mails, documents and any other file formats allowing safely sharing of sensitive information via any media.
- Logging client and server side events in a central database for audit trails and forensic analysis purposes.

## We Enhance Visibility Across Your Entire IT Infrastructure

Netsurion's managed threat protection solution, EventTracker, maintains compliance and increases operational efficiency. EventTracker can be deployed On-Premises for customers who prefer their equipment to reside in their data center. EventTracker is a software-based SIEM and log management solution that resides in a Windows Server environment. EventTracker may also be deployed in a virtual environment using VMware. In both cases, On-Premises installation implies that the EventTracker software resides at the customer's location in some form or fashion. For some customers, the space requirements, staffing issues, or lack of technical expertise make a cloud- hosted solution more attractive, and EventTracker SIEM is deployed in a Tier 1 EventTracker data center.

Netsurion will manage the following:

- Secure Virtual Private Cloud (single tenant) environment
- Installation
- Server disk space
- Platform management
- Windows updates
- Back-up/restore

EventTracker SIEM enables your organization to be aware of potential security risks and internal/external threats that can be identified and eliminated before they are exploited. It guarantees your organization the ability to respond to a security incident and have the necessary data and tools for forensic analysis. The total time required to investigate and mitigate a security incident can be reduced by up to 75 percent, minimizing the potential exposure and costs.

Our experienced staff assumes responsibility for all SIEM related tasks including daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation support and audit support. We augment your IT team, allowing you to focus on the unique requirements of your enterprise, while actively leveraging our expertise.

**Strong Access Control policy and procedures**

EventTracker SIEM enables automatic, unattended consolidation of millions of events in a secure environment along with incrementally scalable to meet the needs of any size organization. It also supports an infinite number of collection points, with each collection point able to process over 100,000 events per second. All this data is identified by the product based Knowledge Base, which contains detailed information on over 20,000 types of events, and automatically determines which logs are alerts, which are incidents, and which can be ignored.

EventTracker platform complies with OWASP guidelines which enforce the product to have a strong authentication and authorization mechanisms to restrict the user access. It incorporates default deny policy bringing more security to customers. It monitors changes on the file system and in the system registry of a Windows system and substantially improves corporate security and availability.

EventTracker SIEM provides customizable, role-based dashboards that allow organizations to control the information visible to a user based on their role in the organization. It also allows users to remove the information they do not want to see, and rearrange the location of the information on the dashboard. For example, a system administrator may only have access to the information on the ten servers they are responsible for maintaining, while the director of security will see the relevant information concerning the entire infrastructure.

EventTracker SIEM monitors all administrators and user's activities for all critical file and folder access on all servers. It monitors successful and failed logon attempts to all servers either locally or remotely. Each EventTracker user has specific user credentials and permissions. With the authentication and authorization mechanism implemented by EventTracker, access privileges are controlled.

**Ease of Deployment and Scalability**

EventTracker Cloud is a highly scalable SIEM and log management solution that offers several deployment options to meet the needs of small organizations with a few dozen critical systems, as well as larger organizations with thousands of systems spread across multiple locations.

Included as a built-in option with EventTracker platform, Behavior Analysis enables you to quickly detect and address changes in system and user behaviors. Automatic baseline learning or flexible rules definitions determine your thresholds for alerting on anomalies in your infrastructure. Real-time processing and correlation give you the complete picture of what's new and different.

### Real-time Monitoring, Account and Configuration Management

The file system and registry of every Windows system is ever-changing. This change may be voluntary or involuntary and happens quickly and often without the user's knowledge.

Change Management is a concept by which all system changes are intelligently tracked and reported on demand for the user to analyze, understand, and if needed, recover from change. EventTracker SIEM alerts you to the critical changes you need to know. EventTracker monitors unauthorized software install / uninstall on all servers. It monitors all the Agents and configuration changes on critical file and database servers. Also enforces system and application policies on critical servers using Change Audit and periodically compare policy. It monitors all security patches and updates to servers.

EventTracker SIEM Change Audit is fully integrated into the EventTracker platform. EventTracker SIEM stores all the change audit data as both system snapshots for later comparisons and as events in EventVault. Change events can have rules written against them to trigger alerts or any other action available in EventTracker SIEM.

### Protect Data and Information

With security as its foremost priority, Netsurion monitors network connections on all windows servers and fire-wall activity. It also monitors for changes or unauthorized access to routers and switches.

EventTracker SIEM is capabilities-rich, with key features that expand its competences beyond SIEM and log management. These include File Integrity Monitoring, Change Audit, Config Assessment, Cloud Integration, Event Correlation, and writeable media monitoring.

The EventTracker platform safeguards data by ensuring stringent rules against unknown authentication and authorization. EventTracker monitors access to file and database servers. Also, it monitors configuration changes on critical file and database servers and alerts the responsible to take further action. EventTracker SIEM also has an optimized, high performance event warehouse that is designed for efficient storage and retrieval of event logs. It reliably and efficiently archives event logs from across the SIEM without the need for any DBMS licenses or other overhead costs. And these logs are compressed and sealed with a SHA-1 signature to prevent potential tampering.

### References:

https://gdpr.eu
https://gdpr.eu/compliance-checklist-US-companies

## How Netsurion Can Help

Not sure where to begin? Netsurion helps you reduce cyber risk, augment your IT team's skills, and spend less time on documentation and compliance readiness. Contact us and our experts can advise you on the path to achieve GDPR preparedness.

## About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's managed platform approach of combining purpose-built technology and a team of cybersecurity experts gives customers and partners the ultimate flexibility to adapt and grow while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.