ONE IDENTITY™

Five things every business needs to know about GDPR

oneidentity.com

After years of preparation and drafting, the final t's were crossed and i's dotted on the General Data Protection Regulation (GDPR) in April 2016, when the Council of the European Union and the European Parliament adopted it. It means that it's time to stop thinking about GDPR and to start acting. Particularly as they will have just two years to become compliant with the new rules on transparency, accountability and data protection.

With the GDPR horizon getting a bit closer every day, we think it's time to highlight five of the most significant aspects of the legislation and how behavior-aware security technologies, like One Identity Safeguard for Privileged Analytics, can help businesses to comply.

1 GDPR in and out of the EU

Although its focus is on the European Union, GDPR does not solely apply to the 28 member states. Instead, the scope of the legislation extends beyond EU controllers and processors to any external organization that has a trading relationship with EU customers.

Additionally, GDPR removes self-assessment as a basis for international data transfer. As such, data exporting organizations that rely on consent to move data outside the EU must now consider whether their data subjects have been informed of the risks of cross-border data flow.

Meanwhile, the European one-stop shop mechanism means that a single set of rules will apply for the whole EU. Thereby easing the associated administrative and financial burden on data controllers and individuals, thanks to cooperation between the data protection authorities of member states.

The introduction of GDPR means sufficient system security is crucial for any business dealing with European data. Not the least because the stakes for failure to keep hackers at bay are about to rise markedly. But these secure environments have to allow for operational maintenance, so that legitimate privileged access users can access the networks that contain the data and work with it.

As such, businesses have to go further than just protecting data through firewalls and the like. They have to keep a keen behavioral monitoring eye on their privileged users—ensuring they are accessing and using data for the right reasons (and are not hijacked accounts).

Controller considerations

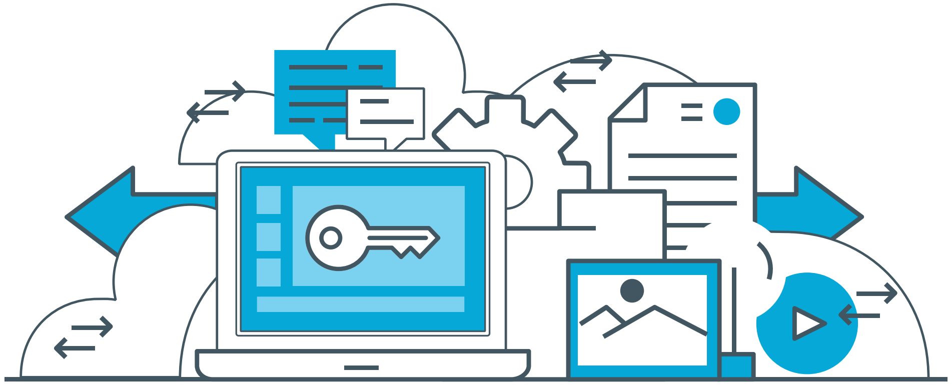
GDPR preserves the concept of personal data processing from Directive 95/46/EC and its corresponding terminology. But it recognizes both contemporary processing complexity and joint controllers—where two or more controllers (businesses) jointly determine the purposes and means of the processing of personal data. Whether acting on the instruction of a third party or alone, the protection of the rights and freedoms of data subjects (as well as the responsibility and liability of controllers and processors) remains untouched.

2 The definition of data

When GDPR kicks in, the definition of the data it governs will change slightly. The two most significant things to consider here are that, as of 25 May 2018, data will cover location and online identifiers; and that the regulation will provide detail on what an 'identifiable person' is—using a test that assesses whether or not data is anonymous.

Alongside this, GDPR is going to define additional specific categories of sensitive data (including genetic and biometric information). And it will add a new concept that doesn't exist under the previous data directive in pseudonymization, which will reduce the chances of an individual being named in a data pool, and will help data controllers to meet their protection obligations.

Because the definition of data is widening, it's likely that organizations will have more privileged access users dealing with it. Having the ability to detect the behavioral anomalies (even if it's as simple as abnormal mouse movement) that indicate a malign presence will become a vital part of any data protection strategy under GDPR.



Implications of GDPR for log management

Because people will be identifiable as data subjects directly and indirectly under GDPR, there are potentially big problems for organizations that collect and manage large amounts of personal data logs (such as email addresses, IP addresses, geolocation, social security numbers, and health-related information).

Similarly, the definitions of anonymous and pseudonymous data, and the technical and organizational measures necessary to de-identify data, could have a profound impact on the way organizations process log data.

For example, data controllers could be exempted from data and portability requests from citizens, should the controllers provide assurances surrounding the ability to re-identify individuals in data sets. There is, however, an exception: flexibility for companies (Article 10):

- ✓ Where a controller is not in a position to identify the individual, the obligations for access, rectification, erasure, right to be forgotten, restriction and data portability do not apply
- ✓ Unless the individual provides additional information enabling his or her identification for exercising these rights
- ✓ Controllers should not refuse to accept additional information provided by an individual in order to support the exercise of his or her rights

3 Processing and compliance

Naturally, the primary concern most organizations will have with GDPR is around processing data and the compliance obligations associated with that.

To ensure compliance, organizations will have to implement appropriate security measures to protect personal data, which may include pseudonymization, encryption and robust key management procedures. As well as ensuring the correct maintenance of documentation, conducting data protection impact assessments that identify risks to data subjects' rights, and implementing data protection principles before processing.

When it comes to reporting, transparency is key. GDPR requires information and notification to be provided in clear and plain language that is easily accessible.

How syslog-ng™ can help

syslog-ng™ Premium Edition and syslog-ng™ Store Box already offer features that help organizations protect personal data contained in logs. Both can store log messages securely in encrypted, compressed, indexed, and time-stamped binary files. So any sensitive data is available only for authorized personnel who have the appropriate encryption key.

De-identifying personal data in log messages can be accomplished using the Pattern Database feature. Based on pre-defined text patterns, personal data such as login credentials can be identified. Once sensitive text is identified, it can be parsed and rewritten. With these features, the parts of log messages containing personal information can be anonymized.

While these features go a long way in protecting private data, they may not always strike the right balance between protecting an individual's right to privacy and securing an organization's IT environment. Anonymization isn't feasible if a security team needs to analyze user activity and respond to suspicious behavior, as a one-way transformation of certain fields will remove any chance of identifying the user.

A way to avoid this situation is to store the original logs in a secure environment and forward the anonymized logs for analysis by the security team. By assigning a unique ID for each log message to both sets of logs, the user can be re-identified. syslog-ng™ can now provide a unique ID for each log message using the use-unique global option. It is generated from the HOSTID and the RCPTID in the format of HOSTID@RCPTID. It has a fixed length: 16+@+8 characters. This method of pseudonymization offers the benefit of enhanced security for the original logs, while retaining the ability of security teams to access the private data only when necessary.

4 Time matters with GDPR

While no organization ever wants to suffer a breach, it's inevitable that some will. Under the forthcoming GDPR rules, there will be strict timeframes around notifying authorities, with organizations required to file as much information as they can provide within 72 hours of becoming aware of a breach.

But it's not only reporting to the authorities that matters. If hacked data is readable, then the organization must also notify data subjects. Because of this focus on accountability, it's going to be necessary for many organizations to designate a Data Protection Officer to keep up with GDPR compliance.

New rules on data rights

One of the rights guaranteed to data subjects under GDPR is a new internet-specific freedom to move their data from controller to controller, when technically feasible to do so, and to request the erasing of their data (without delay) in certain situations.

5 Users need monitoring more than ever

Alongside the encryption of personal data, GDPR requires the restriction of access to personal data. Consequently, controllers and processors have to take technical measures to control access to sensitive data, which should also include some level of user authorization process. Companies will need to protect data in a similar (although slightly less strict) way to how they protect critical infrastructure assets. That means requiring users with access to personal data to be constantly monitored.

Why it pays to act now

GDPR introduces severe sanctions against data controllers and processors who breach the rules, enabling national data protection authorities to impose fines ranging between a maximum of 2% or 4% of annual worldwide turnover; or €20 million. This means that organizations that will be affected by GDPR have no choice but to adapt their processes and systems to secure network components..A vital part of this will be looking at what security technologies can help them to detect behavior that may result in a breach.

By effectively managing privileged access users, as well as analyzing their behavior for tell-tale signs of hacks and hijacks, organizations can go one step further in their data protection efforts. And one step closer to full GDPR compliance.

How Safeguard for Privileged Sessions helps

One Identity Safeguard for Privileged Sessions can be a good fit to meet the requirements set by GDPR. Safeguard for Privileged Sessions is an activity monitoring appliance that controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions.

Central access policy enforcement

Safeguard for Privileged Sessions acts as a centralized authentication and access-control point in your IT environment, which improves data security. The granular access management helps you to control who can access what and when on your data servers.

“Four eyes” authorization

To prevent unauthorized access or human error, Safeguard for Privileged Sessions supports the four-eyes authorization principle. This is achieved by requiring an authorizer to allow administrators to access the server. The authorizer also has the option to monitor the work of the administrator in real-time, as though watching the same screen.

Advanced protection of personal data

Safeguard for Privileged Sessions isolates your data processing systems from unknown intruders or from non-authorized users. In addition, it records all authorized access to sensitive data and provides actionable information in the case of human errors or unusual behavior. It can help to create a data breach report within the required 72 hours.

Prevention of malicious activities

Safeguard for Privileged Sessions monitors privileged activity in real-time and detects behavior anomalies as they occur. In case of detecting a suspicious user action (for example accessing credit card information), Safeguard for Privileged Sessions can send you an alert or immediately terminate the connection.

Tighter employee & data processor control

Safeguard for Privileged Sessions audits “who did what” on systems like your database or CRM servers (for example). It records all sessions in searchable audit trails, making it easy to find relevant information in forensics or troubleshooting situations. You can replay the recorded sessions in your browser or in a separate application just like a movie—all the data processors’ actions can be seen exactly as they appeared on their monitors.

Tamper-proof audit trails

From the Data Protection Regulation perspective, the challenge is similar to log management. User activity records (audit trails) can contain a great deal of personal data, such as passwords, credit card information, client data, and so on. Consequently, companies have to ensure the strict protection of activity records. Safeguard for Privileged Sessions can store the audit trails in a highly confidential way—in an encrypted, time-stamped and digitally signed format, so not even the administrator of this tool can tamper with the audit information. The four-eyes principle can be used for the auditors as well. Safeguard for Privileged Sessions uses multiple keys to encrypt audit trails. In this case, multiple decryption keys are needed to replay the audit trails, so a single auditor cannot access all information about activities and accessed data.

This extreme level of data security—together with granular access rights management - makes Safeguard for Privileged Sessions compliant with the most rigorous laws and national security certifications.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.

Learn more at OneIdentity.com

Learn more

To learn more about commercial and open source One Identity products visit our website:

The syslog-ng homepage:
https://syslog-ng.com

The Safeguard for Privileged Sessions homepage:
https://www.oneidentity.com/one-identity-safeguard/

The Safeguard for Privileged Analytics homepage:
https://www.oneidentity.com/one-identity-safeguard/

Product manuals, guides, and other documentation:
https://support.oneidentity.com/kb-product-select/

ONE IDENTITY™