WHITEPAPER

Impact from the New GDPR:

Countdown to the new EU General Data Protection Regulation (GDPR) has begun, and its Impact will be Global.

The General Data Protection Regulation or GDPR repeals Directive 95/46/EC, and levies crippling penalties for non-compliance. Here's what you need to know about the GDPR, plus 6 guidelines to help you manage the regulation.

The GDPR has been ratified and will go into effect May 25, 2018. Unlike many industry standards, the GDPR centers around a certain geography, the European Union, and the "data subjects" in that geo. Unlike data security standards such as HIPAA (Healthcare data), PCI DSS (credit card data), FISMA (U.S. Government data), GLBA (banking/finance data), and other data security standards, the GDPR will focus on a group of citizens ("data subjects") in a defined geography. The GDPR goes above and beyond securing contact information and a few other data points of the data subjects with whom you have a business relationship. Any of the following items that could possibly identify a data subject must be audited and secured — name, photo, email address, bank details, social media post, medical information, or computer IP address — even if they never become a customer. This qualification adds another layer of complexity to an already-insurmountable information security task – securing your data and all the endpoints connected to it.

Further complicating things are qualifications for age and geography. The GDPR applies to any resident in the EU 16 years of age or older, with a provision for member states, if they choose, to lower the age to 13. Relative to geography, no matter your location, if someone in your organization accesses identifiable data of a "subject," 16 years of age or older, who lives within the EU, as of May 25, 2018, your organization must comply with the standard. The regulation applies when the processing of the subject's data is "related to the offering of goods or services, irrespective of whether a payment of the data subject is required."[1] Some exclusions apply, but the EU has made it clear that the data subject does not have to be a customer. If you handle any data that could identify

[1] https://gdpr-info.eu/recitals/no-80/

the subject, you must comply. The scope of coverage in the GDPR is as disruptive a compliance standard as we have ever seen. The GDPR affects every corner of the globe that looks at, touches, or moves data to/from the EU.

What we're seeing with the GDPR is the government upping the data protection ante by saying industry standards up until now have had little effect in making companies more diligent with protecting its citizens' data. Essentially, the GDPR states that *we're going to create regulation that is enforceable by law, and if you don't comply, the penalties are going to be astronomical* – four percent of annual revenue or €20 million ($22.75 million USD at this writing), whichever is greater, for a multiple offender.

The Origins of the GDPR

> The most notable aspect of the standard is its designation as "regulation," a replacement of the current Directive 95/46/EC adopted in 1995.

The GDPR (General Data Protection Regulation) is official, and the most notable aspect of the standard is its designation as "regulation," a replacement of the current Directive 95/46/EC (a.k.a. Data Protection Directive) adopted in 1995. The Data Protection Directive was designed to provide a single data protection law across the entirety of the EU, something the U.S. has yet to do. The roots of the Data Protection Directive date back to the 1940s when the concept of right to privacy emerged during the UN General Assembly of Paris, 1948. Article 12 of the Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence," and at least one scholar has suggested that the Data Protection Directive is a remnant of the region's wartime past and one country's ability to locate citizens of another based on extensive government records of citizens' personal information.[2] Whatever the motive, by the 1970s European states were convening to discuss an international standard for its citizens' data privacy, and the Data Protection Directive was borne in 1995.

The GDPR extends the Data Protection Directive far beyond the borders of the EU. No matter your geo-location, if someone in your organization accesses identifiable data of a "subject" who lives within the EU, as of May 25, 2018, your organization must comply with the GDPR. Some exclusions apply,[3] but the scope of coverage in the regulation is as disruptive a compliance standard as we have ever seen. The GDPR affects every corner of the globe that looks at, touches, or moves certain identifiable data to/from the EU.

What to Watch for with the GDPR Compliance

There are 11 Chapters and 99 Articles in the GDPR. The PDF from the Official Journal of the European Union spans 88 pages. CorreLog has reviewed the regulation and highlighted eight items from it to be on your radar as you prepare for the compliance auditing you will need.

1. Data File Types: It took the EU Parliament four years of preparation (and debate) to approve the GDPR on April 14, 2016. The GDPR applies to any organization that "offers goods or services to, or monitor the behavior of EU data subjects," regardless of the company's location.[4] Since the regulation centers around a "data subject" and

[2] http://jtl.columbia.edu/wp-content/uploads/sites/4/2014/05/52ColumJTransnatlL569_Practicing-Privacy-Online_Examining-Data-Protection-Regulations-Through-Googles-Global-Expansion.pdf
[3] http://www.privacy-regulation.eu/en/2.htm
[4] http://www.eugdpr.org/

geography, your organization will have to audit any user who has access to files that can be used to identify the subject directly or indirectly – name, photo, email address, bank details, social media post, medical information, or computer IP address. The magnitude of systems and applications this metadata touches will make the GDPR auditing a very comprehensive undertaking.

2. Appointing a DPO: The EU Parliament believes this is no task to be taken lightly, and depending on your organization type, you may be required to appoint a Data Protection Officer or DPO. The GDPR provides that you must appoint a DPO if your organization falls into one of the following categories: "(a) public authorities, (b) organizations that engage in large-scale systematic monitoring, or (c) organizations that engage in large-scale processing of sensitive personal data (Art. 37)."[5]

3. Processing Child Data: Parental consent is required to process personal data of children under the age of 16. Member states have the option to reduce this age limit but not below 13 years old. If member states change the age minimum, it will just add another layer of auditing complexity to what you need to watch for.

Photo courtesy of Andy Roth, USA.

4. Data Breach Reporting Time-frame: GDPR Article 33 states that in the case of breach "the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55…" Other than the obviousness of 72-hour time-frame, it should be noted that the GDPR recognizes two functions within your organization that need breach visibility – the "Controller" and the "Processor." The Controller generally determines purpose, conditions, and means of data processing, while the Processor is naturally the computation entity acting on behalf of the Controller.

5. Processing Activity for Goods or Services: The GDPR stipulates that the regulation applies to all firms that offer goods and/or services to EU residents whether or not a payment is transacted. If you market your goods/services to any EU organization, the GDPR applies to both customers and prospects in your contacts list.

6. Subjects' Legal Right to be Forgotten: Citizens under the protection of the GDPR have the "right to obtain from the Controller the erasure of personal data concerning him/her without undue delay and the Controller shall have the obligation to erase personal data without undue delay…" There are stipulations (and exemptions) here too numerous to detail[6]; the point to be made is you must have a method for data subjects to request erasure and the request should include all instances of subjects' data, including archives.

The data subject has the right to know what data has been collected concerning him/her. The standard is vague on time-frames to provide this information to subjects, so it may be to your advantage to review this and other parts of the regulation with your legal team that are not clear.

[5] http://www.privacy-regulation.eu/en/37.htm

[6] http://www.privacy-regulation.eu/en/17.htm

7. Transfer of Personal Data to Third-party Countries: Article 44 of the GDPR addresses the "transfer of personal data which are undergoing processing or are intended for processing after transfer," acknowledging that the transfer of data is normal for conducting international trade. In another area of vagueness, the regulation merely states (in multiple recitals) that "all provisions…shall be applied to ensure that the level of protection is not undermined." Again, you may want your legal team to be aware of your organization transferring subjects' data to other countries outside the EU.

8. What is the Impact to Bottom Line? Non-compliance to the GDPR regulation can result in fines up to four percent of global annual revenue, with a cap set at €20 million ($22.4 million USD at this writing). Penalties accrue on a scaling model where the four percent/€20 million cap is the max penalty. The lower-level fine is set at the two-percent-of-revenue (previous year) mark or €10 million, whichever is higher. Fines will be administered by individual member states. A list of criteria for fines determination can be found on the GDPR EU site here - http://gdpreu.org/compliance/fines-and-penalties/.

6 Things to Help Prepare for GDPR Day 1, May 25, 2018.

The GDPR, at 88 pages, is not as overwhelming to comprehend as NIST's supplemental documentation (Special Publications and Federal Information Processing Standards) for the United States' standard, the Federal Information Security Modernization Act or FISMA; these supplements tally more than 1,000 pages. Supplemental documents for helping us understand the GDPR such as NIST's SPs and FIPS could be on the roadmap, we just don't know at this point; we are early on with the regulation. What is clear is that the GDPR will be different. Because of the punitive nature of the GDPR, it has the potential to be significantly disruptive of overall enterprise business strategy (it directly affects the bottom line), and not merely an IT discipline as cyber-security has been over the years. The initial fines falling under the GDPR will have a ripple effect across global markets, and unless preparation is taken now, there will be a mad scramble for enterprises to retroactively bring their workforces into compliance. When it comes to data security and its accompanying compliance, you're only as strong as your weakest threat vector.

The following 6 things will help your GDPR compliance as you continue your journey to zero hour, May 25, 2018.

1. Have Security Information and Event Management visibility from all sources

To keep tabs on your data and who's accessing (or even looking at) your data, you need a 360-degree view of all user activity surrounding your data. At the heart of this security information and event management or SIEM practice is log management in conjunction with event correlation. Collecting event logs from endpoint devices, firewalls, routers/switches, desktops, servers, and applications (log management), and then correlating them against norms of user behavior (events) are the basics of SIEM. It is much more complicated than that but the idea is to understand the norms of user interactions with your network data – i.e. 99 percent of the time Bill logs in between 8:00 a.m. and 8:30 a.m. from his normal IP address in Boston, and logs off before 6:00 p.m. Correlating this normal behavior to, say, five logins at 2:00 a.m. from an IP address in Saudi Arabia, when you know Bill is in

Boston, is an anomaly and should be investigated immediately with appropriate action taken. And you must do this event log correlation across all platforms, including Windows, mainframe, Linux, UNIX, and other open systems.

The metadata surrounding GDPR – name, photo, email address, bank details, social media post, medical information, or computer IP address – can quickly balloon your log data to levels that slow systems resources. Your correlation engine does not need all the log data so you will want a tool that has efficient indexing and filtering. CorreLog's SIEM Correlation Server is such a product and you can find out more information at CorreLog.com.

2. Reinforce your endpoint threat vectors

You are also going to need sufficient end-point management that fortifies the security of your enterprise mobility management systems, or EMMs. Your mobile workforce occupying the far reaches of your perimeter, outside the physical walls of your organization, bordering your countries of incorporation, may just be the most vulnerable threat vector to the data protected by the GDPR. As stated earlier, the GDPR is not confined to the EU, it is a global data security regulation. Your enterprise's EMM is a separate infrastructure with its own operating system. Your EMM system is a great tool for provisioning and managing devices but it was never designed to be enterprise security. For this you must include your endpoint event logs into your SIEM, providing visibility to all user events from all computing sources rolled up into your IT Security Operations Center, or SOC.

This will be especially important for teams overseas and any users that travel overseas. We live and work in a globally-connected world and you need visibility to user activity outside your network perimeter as much as any other group of people in your organization.

3. EMM & SIEM integration to your IT SOC

All this event logging and event correlation must to be rolled up into a single view of data security truth within your IT Security Operations Center. Securing your data means knowing and visualizing the user interactions to your data in real time. Theoretically, we will never be able to build a hack-proof data store because humans are mistake-prone. The latest Verizon DBIR[7] reveals that 81 percent of hacking-related breaches leveraged stolen and/or weak passwords. Security industry pundits agree that breach is inevitable and the focus should be on real-time threat visibility with instantaneous notifications of a breach, followed immediately by corrective action to stem the bleeding. (The EU, with the GDPR believes this too!) What makes this all possible is a security policy based on 100 percent visibility of the activity across all the threat vectors in your network in your SOC.

Where the GDPR is concerned, this visibility will give the Controller a path to validate the technical and organizational measures they are undertaking to maintain compliance and in the event of breach, plus an audit trail of forensics with which to determine the who, what, when and where of the breach.

4. Real-time alerting system because of GDPR Article 33

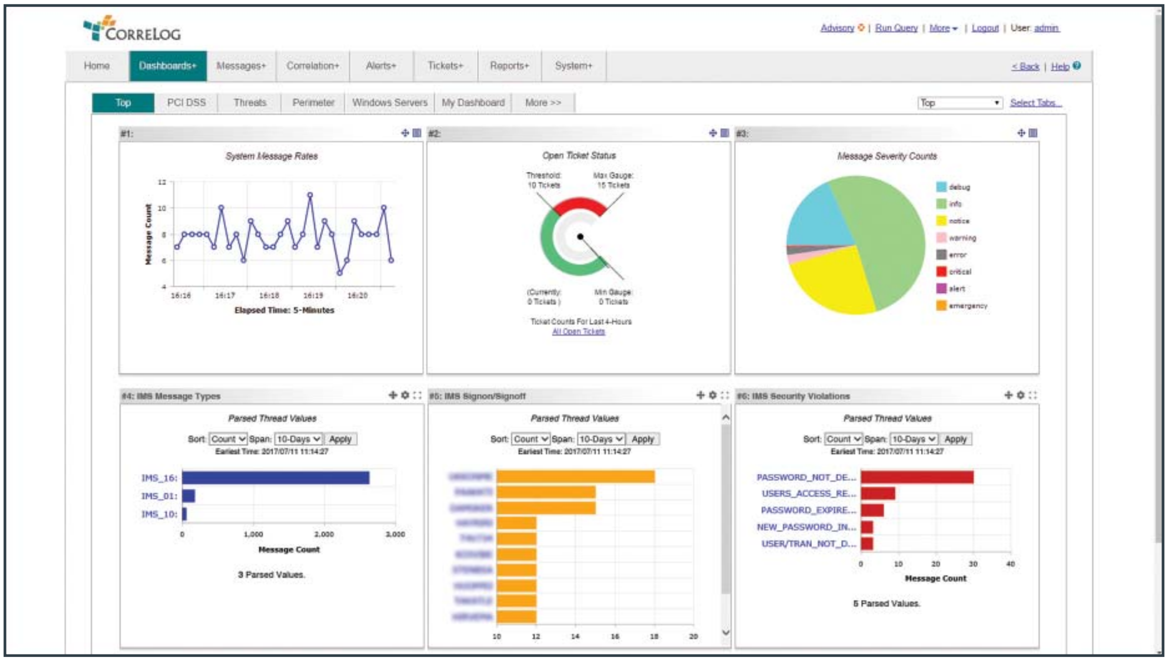
Article 33 of the GDPR states that "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to

[7] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

the supervisory authority competent in accordance with Article 55,[8] unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Essentially, you need real-time alerting across all threat vectors because in the world of cyber-crime, 72 hours is not that long, considering the average time to discover a breach (according to the latest IBM/Ponemon Institute *"2017 Cost of Data Breach Study"* [9]) is still a staggering 191 days. It is not out of the ordinary for some mainframe systems to issue reports on user activity every few days; these are called batch reports. Clearly, as far as information security (InfoSec) and now the GDPR, real-time visibility and notifications on anomalous user behavior is paramount and could be the difference in millions of dollars of fines.

CorreLog is one of the only mainframe security vendors that offers a software-based InfoSec system that will send real-time alerts to a SIEM system or SOC. The product is called CorreLog zDefender™ and it uses facilities already built into IBM z Series (including the new z14) mainframes to send up-to-the-second alerts to InfoSec personnel when anomalous user behavior is detected. zDefender™ holds certified integrations with the world's leading SIEMs including QRadar, ArcSight, RSA Security Analytics, and McAfee ePO, and also field integrations with SIEMs such as Splunk, LogRhythm, Dell SecureWorks, and others. In addition to the ability to send real-time alerts about potential breach, it's a good idea to have a system that can trigger an event into your service desk.



For mainframe data security auditing, CorreLog offers its dbDefender™ product for both of IBM's DB2 and IMS database products.

[8] Article 55 addresses the competence of the supervising authority.

[9] https://www.ibm.com/security/data-breach/

5. Alerting system that can trigger an enterprise Service Desk

Automation is everything when answering the call for Infrastructure and Application Service Delivery. Every CIO has a service-level percentage to maintain and failure to comply can compromise organizational productivity and in turn, profitability. All systems must be “go” (near) all the time when it comes to performance and availability of manufacturing, HR, communications, and other vital systems that keep an organization’s people up and running.

The Service Desk or Helpdesk has been instrumental in bringing visibility to Infrastructure and Application service levels. The second an application or asset that an application is dependent upon is interrupted, an automated helpdesk ticket can be logged into a Service Desk system and immediate remediation can be undertaken. The app can be transferred to a redundant server or other automated response can be taken to ensure systems outage is minimized.

Given the 72-hour time requirement for GDPR breach reporting, we need to bring this Service Desk notification system into the realm of IT security and compliance. Your EMM and SIEM processes that are populating the IT SOC with real-time data need to have the capability to at least issue a trigger to a notification system that a potential breach needs to be investigated. In addition to a help-desk trigger, an automated email or SMS text should also be generated to security admins to shut down ports or other immediate remediation action, either manual or automated.

6. Get your legal team involved now.

Navigating the GDPR is undoubtedly going to take you through uncharted legal waters. The GDPR represents some of the most stringent data protection laws in the world and for the first time we are seeing a “data protection standard” mentioned alongside “fundamental rights.”[10] The EU geographically is relatively small and has more than 30-member states, each permitted to legislate the GDPR differently. This variation of understanding of what will be permitted by member state, coupled with comprehension of the regulation’s language should be enough to trigger legal team involvement now. On top of that, there is little (if any!) precedent of a four percent fine from a data standard managed by a confederation of EU member states. How will the GDPR be enforced? What recourse will you have when you go to mediation or trial? These are just a few of the agenda items for your legal team to be wrangling with now as we approach May of 2018.

What’s next?

In the technology world, the word “disruptive” is thrown out in abundance to describe a lot of concepts said to alter the way we conduct business-as-usual. Some of this labeling is accurate, but it is often an overused term to add hype to a new product or service. In contrast, the GDPR will absolutely be a very disruptive piece of regulation that your organization – whether based in the EU or not – will have to navigate around.

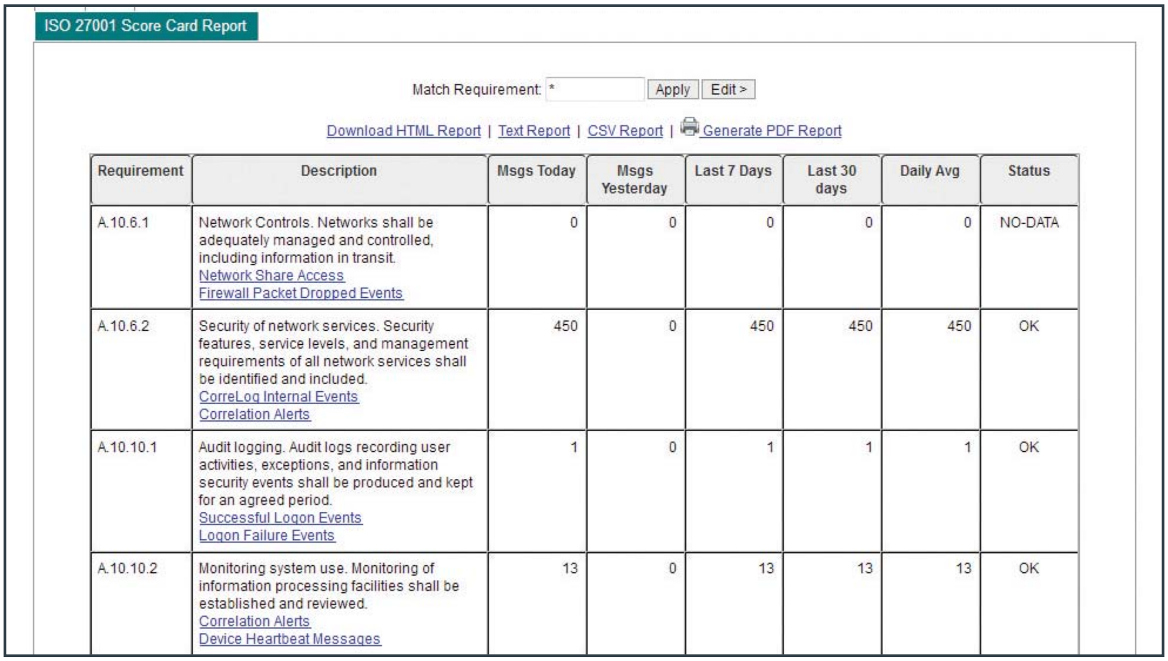
If your organization is US-based and you only make a single phone call next year to an EU-based prospect, and your notes about the conversation go into your CRM system, you could be subject to the constraints of the regulation. This regulation affects the entire planet, regardless of where the data processing takes place.

Many of you with a best-practice approach to IT security and compliance won’t need to change your approach that much at all. For those of you in this group, just stay the course.

[10] https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/home/

For those of you still struggling with enterprise-wide visibility to user activity, privileged or otherwise, this whitepaper is designed as an educational tool with some best-practice guidelines for helping your organization manage GDPR compliance. CorreLog can be a valuable resource for a single repository of event log data across all systems, mainframe and distributed, with the visibility to stay out in front of any trouble the GDPR may bring. But you need to start planning now, striving to have the ability to see anomalous behavior as it occurs in real time, and most importantly, the ability to alert appropriate security personnel on the fly for any perceived threat.

Since 2008, CorreLog has been helping clients with data security and compliance auditing with best-in-class software solutions. We have a proven track record of securing data across both mainframe and Windows/UNIX systems in a multitude of industries including Banking/Finance, Healthcare/Insurance, Retail, CPG, and Government. For more information on CorreLog solutions, please visit www.CorreLog.com.



ISO 27001 Score Card Report

Match Requirement: * Apply Edit >

Download HTML Report | Text Report | CSV Report | Generate PDF Report

Requirement	Description	Msgs Today	Msgs Yesterday	Last 7 Days	Last 30 days	Daily Avg	Status
A.10.6.1	Network Controls. Networks shall be adequately managed and controlled, including information in transit. Network Share Access Firewall Packet Dropped Events	0	0	0	0	0	NO-DATA
A.10.6.2	Security of network services. Security features, service levels, and management requirements of all network services shall be identified and included. CorreLog Internal Events Correlation Alerts	450	0	450	450	450	OK
A.10.10.1	Audit logging. Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period. Successful Logon Events Logon Failure Events	1	0	1	1	1	OK
A.10.10.2	Monitoring system use. Monitoring of information processing facilities shall be established and reviewed. Correlation Alerts Device Heartbeat Messages	13	0	13	13	13	OK

About CorreLog

CorreLog, Inc., a privately held corporation, is an independent Security Information & Event Management (SIEM) software vendor that has produced software and framework components used successfully by hundreds of private and government organizations worldwide. Our core solutions provide visibility across both mainframe and distributed systems on user activity that is indicative of cyber threat. Since 2008, CorreLog, Inc. has been committed to delivering better decision-support solutions for InfoSec and security auditing professionals who need more advanced perimeter security and improved adherence to PCI DSS, GDPR, HIPAA, SOX, IRS Pub. 1075, GLBA, FISMA, NERC, ISO 27001, and other industry standards for securing data. Our solutions are designed to be highly interoperable and complementary to clients' existing IT investments.

We consider our technology approach to be unique in both personnel and product, and we believe our solutions pass the test of low total cost of ownership with high SIEM functionality. For more information on CorreLog products, please visit www.CorreLog.com.

CorreLog.com

CorreLog, Inc.
1004 Collier Center Way, 1st Floor
Naples, Florida 34110
1-877-267-7356 Toll-free (US only)
+1-239-514-3331 International
info@CorreLog.com