

Home (<http://www.corporatecomplianceinsights.com/>)

Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

Featured (<http://www.corporatecomplianceinsights.com/category/featured/>)

Technical Requirements for GDPR Compliance



For GDPR Compliance, Take These Steps

If you're not already compliant with the General Data Protection Regulation (GDPR), you're already behind the 8 ball. But don't despair; your organization can get up to speed, one step at a time. Maxine Henry outlines a step-by-step approach to GDPR compliance and discusses the importance of policy management.

Compliance with the European Union General Data Protection Regulation (GDPR) has a lot of organizations up in arms — but does yours need to be one of them?

Yes, the GDPR is a weighty mandate, with 99 controls (<https://www.eugdpr.org/>), and harsh penalties for those who don't comply: up to 4 percent of your organization's global annual revenues or €20 million, whichever is greater, plus untold damage to your brand.

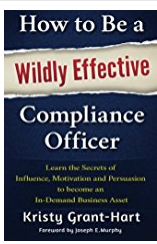



But GDPR compliance (<http://www.corporatecomplianceinsights.com/frameworks/gdpr-compliance/>), isn't impossible, and it needn't be overwhelming — not if you have a clear intention of boosting your organization's data privacy practices as the regulation requires. To start, you must first take a hard look at your organization's policies and procedures.

Having the right policies and procedures in place is key to GDPR compliance. Why? Because your written, shared standards form the backbone of your enterprise. Your business will only stand as tall and strong as they allow, guiding all your people to a singular goal: the organization's success. And if you want to succeed in business from now on, you'll need to comply with the GDPR.

How do your policies stand against the GDPR's controls? Keep these requirements in mind as you revise your policies or write new ones, from the drafting stage all the way through editing, approving, updating, distributing, implementing, training, documenting, updating, maintaining and auditing.

What is your privacy policy, for instance? The GDPR's reason for being is to protect EU citizens' privacy. How do you present your enterprise's privacy policy to customers and employees? Can they read it easily and understand what it means? If it's long and full of legal jargon, you will need to re-write it. The GDPR requires privacy policies to be clear and succinct. (<https://gdpr-info.eu/art-7-gdpr/>)

CCI Recommends:

 <p>How to Be a Wildly Effective Compliance Officer: Learn the Secrets of Influence, Motivation and Persuasion to Become an In-Demand Business Asset Kristy Grant-Hart Foreword by Joseph V. Scarpino</p> <p>How to Be a Wildly Effective Compliance Officer: Learn... (http://aax-us-east.amazon-adssystem.com/x/c/QqP00...) Effective-Compliance-Officer-</p>	 <p>Compliance Management: A How-to Guide for Executives, Managers and Other Compliance Professionals Debbie Troklus, PhD, and Sheril Vacca</p> <p>Compliance Management: A How-to Guide for Executives... (http://aax-us-east.amazon-adssystem.com/x/c/QqP00...) Management-How-Executives-</p>	 <p>Compliance 101, Fourth Edition Debbie Troklus & Sheril Vacca</p> <p>Compliance 101, Fourth Edition (http://aax-us-east.amazon-adssystem.com/x/c/QqP00...) 101-Fourth-Debbie-Trokus/do/0991078381/ref...</p>	 <p>COMPLIANCE: A CONCISE GUIDE TO THE ROLE OF THE COMPLIANCE FUNCTION IN FINANCIAL SERVICES FIRMS Daniel S. Lewis</p> <p>Compliance: A concise guide to the role of the Complia... (http://aax-us-east.amazon-adssystem.com/x/c/QqP00...) concise-Function-financial-services/do/1534778381/r...</p>
--	---	---	--

All Search Amazon Go

Ads by Amazon (http://aax-us-east.amazon-adssystem.com/x/c/QqP001HzPVZESXBKuv5uXBBoAAAFIAK22lgEAAAFKAdFsUBc/https://affiliate-program.amazon.com/home/ads/ref=sm_n_ma_dka_US_logo?adId=logo&creativeASIN=logo&linkId=5a5e8792ed59e2799b4ef7d3e47258b4&tag=cci06-20&linkCode=w43&ref-refURL=http%3A%2F%2Fwww.corporatecomplianceinsights.com%2Ftechnical-requirements-gdpr-compliance%2F&slotNum=0&imprToken=.8pr9qfv4KARO76ACuui1g&adType=smart&adMode=manual&adFormat=grid&impressionTimestamp=153331ms-src=nsa-ads&cid=nsa-ads)
(http://aax-us-east.amazon-adssystem.com/x/c/QqP001HzPVZESXBKuv5uXBBoAAAFIAK22lgEAAAFKAdFsUBc/https://www.amazon.com/adprefs/ref=sm_n_ma_dka_US_ac?t20&linkCode=w43)

Do you have specific, unambiguous policies for handling, tracking, storing and sharing the data you collect? Do your employees know what they are? Have you defined each step in the process, including how to tag data so your company can easily retrieve it after sharing it with a third party? The GDPR requires you to erase, on request, any EU citizen data (<https://gdpr-info.eu/art-17-gdpr/>), you have collected and for all entities you have shared it with to do the same. How will your organization comply with this mandate?

The Next Step: THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL



(<http://www.corporatecomplianceinsights.com/>)

Once you've got the proper policies in place, you'll need to determine which of them your enterprise complies with and in which areas you fall short, as well as what you must do to fully adhere to the rules you have set. This stage, *policy management*, is too often overlooked or given short shrift — and that is a mistake. Because all the rules in the world will do you no good if you are not abiding by them. Without good policy management, your organization could fall out of GDPR compliance even after you have worked so hard to get there — and you might not even realize it until it's too late.

For successful policy management:

1. Build a policy management system.
2. Take a risk-based approach (<https://iapp.org/news/a/demystifying-the-risk-based-approach/>), to building policies and procedures.
3. Automate as much as possible.
4. Maintain a consistent format across all policies and procedures.
5. Maintain a system of record for reporting and auditing.
6. Restrict changes to policies and procedures to applicable staff.
7. Link all documents to GDPR principles.

At the end, you should have a policy inventory (<https://www.policymedical.com/how-to-complete-a-policy-inventory/>), with detailed information about each policy and which GDPR controls it addresses and how. You must also make sure to update your policies whenever the GDPR changes or other new industry requirements come along, and you must make sure employees have access to the latest versions — including translations for international audiences.

Every step in the policy process is important for ensuring that your organization is GDPR compliant. Best practices for managing that process include:

- **Training and Communication** – You must train all your employees on your enterprise's GDPR policies and procedures.
- **Attestation and Certification** – Employees must sign off on policies, and those acknowledgement forms must be tracked and accessible in case your business gets audited or sued.
- **Enforcement**. How will your enterprise handle reports of wrongdoing? Investigating alleged infractions promptly and enforcing the rules is the best way to communicate your commitment to GDPR compliance — both to regulators and internally.
- **Metrics and Performance Improvement** – How will your organization track incident reports? How will you determine which policies and procedures need to be modified, updated or retired? How will you track investigations? How will you know if your employee training is working? How will you ensure that all employees have signed acknowledgment forms, and will you be able to promptly demonstrate that? Make sure you have processes in place to measure how well your policy management process is working and to continually improve.

- ■ **Correction** – Not all policies and procedures are created equal. Some, you may find, don't work as they should. Establish a policy management program with policies that are not effective and for resolving them. (http://www.corporatecomplianceinsights.com/)

One Step at a Time

By now, you may be feeling overwhelmed. That's understandable. The GDPR is a comprehensive law with many requirements.

Full compliance is attainable, however. Here's a step-by-step approach to help you get there:

- Conduct a risk assessment to identify your policies, procedures and risks across the enterprise.
- Consider budgeting for policy management software, storage, GRC, staff and other resources.
- Harmonize and map the GDPR's controls based on standard frameworks and existing compliance controls.
- Automate your policy management to save time and reduce costs.
- Track attestations consistently and keep records in one place for ready retrieval in the event of legal action.
- Consider how you can use policy management tools to meet third-party and auditor needs.
- Make sure the processes and program you build will be auditable and will stand over time.

Do you see a recurrent theme in this list? Automation tools can do much of the work of GDPR compliance for you.

The GDPR is here to stay, and pretty much every enterprise doing business online — and some that don't — will need to comply with its mandates. The bad news is, it's a big and complex law, and it's taking effect very soon. The good news, however, is that the problem technology has created — data privacy protection — it can also help resolve, freeing you to focus on what matters: your customers.

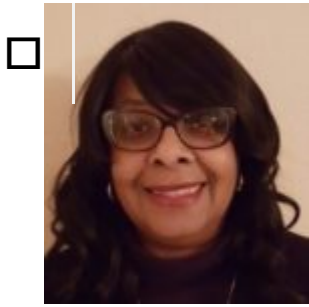
(https://shareasale.com/r.cfm?b=688002&u=1751538&m=57041&urlink=&afftrack=)

Maxine Henry

(http://www.corporatecomplianceinsights.com/author/maxine-henry/)

Maxine Henry is a GRC expert at Reciprocity. She is actively engaged with helping customers take a holistic approach to governance, risks and compliance.

Maxine has consulted at major firms including The Walt Disney Company, Cylance, Experian and Hyundai Autoever America. Her accomplishments and skills include governance, risk and compliance cybersecurity; data privacy and protection; e-discovery and General Data Protection Regulation (GDPR). She has helped clients strategically and tactically with developing technical and compliance solutions.



(<http://www.corporatecomplianceinsights.com/>)

[Previous Post \(http://www.corporatecomplianceinsights.com/update-wan-strategy-secure-company-network/\)](http://www.corporatecomplianceinsights.com/update-wan-strategy-secure-company-network/)
[Next Post \(http://www.corporatecomplianceinsights.com/vice-president-risk-management-phoenix-arizona/\)](http://www.corporatecomplianceinsights.com/vice-president-risk-management-phoenix-arizona/)

RELATED POST



Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

(<http://www.corporatecomplianceinsights.com/>)

(<http://www.corporatecomplianceinsights.com/asia-pacifics-anti-corruption-rankings-2016/>)

Asia-Pacific's Anti-Corruption Rankings for 2016

(<http://www.corporatecomplianceinsights.com/asia-pacifics-anti-corruption-rankings-2016/>)

Posted by **Wendy Wysong** (<http://www.corporatecomplianceinsights.com/author/wendy-wysong/>) - February 20, 2017 0 (<http://www.corporatecomplianceinsights.com/asia-pacifics-anti-corruption-rankings-2016/#respond>)

Scores Run the Gamut Each year, Transparency International publishes the Corruption Perceptions Index, a ranking of the world's nations according...



Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

(<http://www.corporatecomplianceinsights.com/>)

(<http://www.corporatecomplianceinsights.com/compliance-officers-need-independence/>)

Why Compliance Officers Need Independence

(<http://www.corporatecomplianceinsights.com/compliance-officers-need-independence/>)

Posted by **Donna Boehme** (<http://www.corporatecomplianceinsights.com/author/donna-boehme/>) - February 17, 2017 0 (<http://www.corporatecomplianceinsights.com/compliance-officers-need-independence/#respond>)

“Collaboration, not Subordination” Captive compliance programs are hamstrung programs. Compliance officers who enjoy independence and are able to collaborate with...



Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

(<http://www.corporatecomplianceinsights.com/>)

(<http://www.corporatecomplianceinsights.com/compliance-trump-era-markers-placed/>)

Compliance in Drumpf Era: More Markers Placed

(<http://www.corporatecomplianceinsights.com/compliance-trump-era-markers-placed/>)

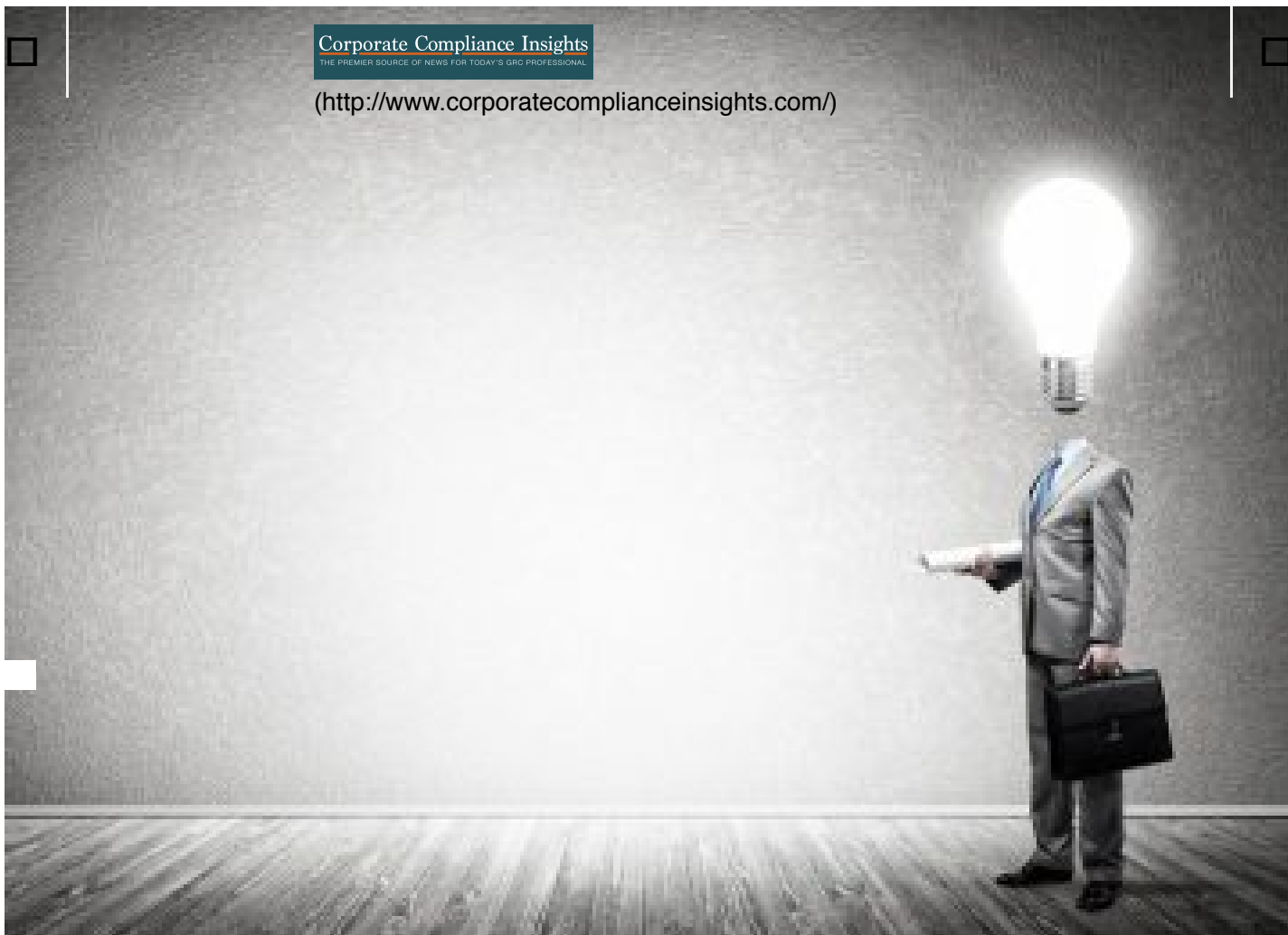
Posted by **Matt Kelly** (<http://www.corporatecomplianceinsights.com/author/matt-kelly/>) - February 14, 2017
□ 0 (<http://www.corporatecomplianceinsights.com/compliance-trump-era-markers-placed/#respond>)

Predictions

on the FCPA Front The U.S. government is in a state of flux; with a new President comes a...

Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

(<http://www.corporatecomplianceinsights.com/>)



(<http://www.corporatecomplianceinsights.com/cognition-became-weapon/>)

How Cognition Became a Weapon

(<http://www.corporatecomplianceinsights.com/cognition-became-weapon/>)

Posted by **James Bone** (<http://www.corporatecomplianceinsights.com/author/james-bone/>) - February 8, 2017

□ 0 (<http://www.corporatecomplianceinsights.com/cognition-became-weapon/#respond>)

The Trust Conundrum Users' trust in the internet increases with greater usage. On the flip side, as internet usage increases,...



(<http://www.corporatecomplianceinsights.com/artificial-intelligence-skilled-professionals-need-one-another/>)

Artificial Intelligence and Skilled Professionals Need One Another (<http://www.corporatecomplianceinsights.com/artificial-intelligence-skilled-professionals-need-one-another/>)

Posted by **Robert Clyde** (<http://www.corporatecomplianceinsights.com/author/robert-clyde/>) - February 3, 2017

□ 0 (<http://www.corporatecomplianceinsights.com/artificial-intelligence-skilled-professionals-need-one-another/#respond>)

Limiting Risks in Adopting AI Enterprises and consumers are poised to adopt artificial intelligence in 2017. But along with many...



(<https://www.facebook.com/CorporateComplianceInsights/>)



(https://twitter.com/ccli_compliance)



linkedin.com/company-beta/366574)

(http://www.corporatecomplianceinsights.com/)



(http://feeds.feedburner.com/CorporateComplianceInsights)

SITE SEARCH

Search ...



SUBSCRIBE



(http://www.corporatecomplianceinsights.com/subscribe/)



(http://bit.ly/18CEI)

PODCASTS

TRACE Podcast: Harmonizing Global Settlements
(http://www.corporatecomplianceinsights.com/trace-podcast-harmonizing-global-settlements/)



August 2, 2018

Corporate Compliance Insights

THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

[\(http://www.corporatecomplianceinsights.com/\)](http://www.corporatecomplianceinsights.com/)

Measuring Onboarding Effectiveness

[\(http://www.corporatecomplianceinsights.com/measuring-onboarding-effectiveness/\)](http://www.corporatecomplianceinsights.com/measuring-onboarding-effectiveness/)

July 31, 2018



TRACE Podcast: Duke Cunningham and the Bribe Menu

[\(http://www.corporatecomplianceinsights.com/trace-podcast-duke-cunningham-bribe-menu/\)](http://www.corporatecomplianceinsights.com/trace-podcast-duke-cunningham-bribe-menu/)

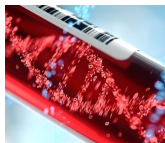
July 25, 2018



TRACE Podcast: UN Office on Drugs and Crime

[\(http://www.corporatecomplianceinsights.com/trace-podcast-un-office-drugs-crime/\)](http://www.corporatecomplianceinsights.com/trace-podcast-un-office-drugs-crime/)

July 18, 2018



TRACE Podcast: "Bad Blood" – The Theranos Scandal

[\(http://www.corporatecomplianceinsights.com/trace-podcast-bad-blood-theranos-scandal/\)](http://www.corporatecomplianceinsights.com/trace-podcast-bad-blood-theranos-scandal/)

July 11, 2018

VIDEOS



Thomson Reuters: Bank Culture Reform

[\(http://www.corporatecomplianceinsights.com/thomson-reuters-bank-culture-reform/\)](http://www.corporatecomplianceinsights.com/thomson-reuters-bank-culture-reform/)

April 30, 2018



Third-Party Due Diligence Requirements for Financial Institutions

[\(http://www.corporatecomplianceinsights.com/third-party-due-diligence-requirements-financial-institutions/\)](http://www.corporatecomplianceinsights.com/third-party-due-diligence-requirements-financial-institutions/)

March 20, 2018



The Impact of Technology on Enhanced Due Diligence

[\(http://www.corporatecomplianceinsights.com/impact-technology-enhanced-due-diligence/\)](http://www.corporatecomplianceinsights.com/impact-technology-enhanced-due-diligence/)

August 3, 2017



U.S. Regulatory Examiners' 2017 Priorities

[\(http://www.corporatecomplianceinsights.com/u-s-regulatory-examiners-2017-priorities/\)](http://www.corporatecomplianceinsights.com/u-s-regulatory-examiners-2017-priorities/)

February 6, 2017

SCOTUS Decides Highly-Anticipated Insider Trading Case

[\(http://www.corporatecomplianceinsights.com/scotus-decides-highly-anticipated-insider-trading-case/\)](http://www.corporatecomplianceinsights.com/scotus-decides-highly-anticipated-insider-trading-case/)

December 22, 2016

Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GC&O PROFESSIONAL

(http://www.corporatecomplianceinsights.com/)



(https://shareasale.com/r.cfm?)

b=907428&u=1751538&m=67568&urlink=&afftrack=)



(https://shareasale.com/r.cfm?)

b=238894&u=1751538&m=26342&urlink=&afftrack=)



Corporate Compliance Insights
THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

(http://www.corporatecomplianceinsights.com/)

(http://www.corporatecomplianceinsights.com/compliance-

job-interview-questions-and-answers/)

ABOUT CCI

Corporate Compliance Insights is a professionally designed and managed forum dedicated to online discussion and analysis of corporate compliance, risk assessment, ethics, audit, and corporate governance topics. Additionally, CCI is a focused knowledge-sharing forum designed to educate and encourage informed interaction within the corporate compliance community.



(https://www.facebook.com/CorporateComplianceInsights/)



(https://twitter.com/cci_compliance)



(https://www.linkedin.com/company-beta/366574)



(http://feeds.feedburner.com/CorporateComplianceInsights)

We are a participant in the Amazon Services LLC Associates Program, an affiliate advertising program designed to provide a means for us to earn fees by linking to Amazon.com and affiliated sites.

CCI Privacy Policy (<http://www.corporatecomplianceinsights.com/privacy-policy/>)

©2017 Corporate Compliance Insights