Two Years In, IT Thought Leaders Judge GDPR's Impact

By: Chris Preimesberger, eWEEK (/Authors/chris-preimesberger) | Updated May 25, 2020

eWEEK ANALYSIS: Has the General Data Protection Regulation enacted by the European Union on May 25, 2018, had the effect that originally was intended to keep personal and business data safe for e-commerce and communication? eWEEK asked the question, and we received a lot of perspectives. Read them here.

It’s been exactly two years since the General Data Protection Regulation, or GDPR, was put into force by the European Union on May 25, 2018.

eWEEK has covered (https://tinyurl.com/GDPR-CP-eWEEK) the genesis, institution and passage of this pioneering international data privacy law since long before that date became a milestone in data protection and privacy history. Take a look at our list of articles on this topic (https://tinyurl.com/GDPR-eweek) to understand why this legislation is so important to the world’s IT business and international commerce in general.

Here's the official statement from the European Union (https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_20_913) on the significance of the GDPR on its second anniversary.

At the one-year mark in 2019 (https://www.eweek.com/security/gdpr-one-year-anniversary-data-privacy-still-needs-help), the consensus was that GDPR was simply the first pitch in the first inning of an international campaign to safeguard personal and business data like it had never been safeguarded before. The work has started against the bad IT actors in the world, and it won’t be completed any time soon.

Further reading

GDPR at Age 2: Nothing has Changed, yet Everything... (/security/gdpr-at-age-2-nothing-has-changed-yet-everything-has-changed)

How Using AI Vastly Improves Threat Detection (/security/how-using-ai-vastly-improves-threat-detection)

More regulations are coming: California's Consumer Protection Act of 2018 went into effect Jan. 1, 2020, and several other U.S. states are expected to follow suit this year and next. CCPA makes nationwide organizations protect California residents' personal data, and subsequent laws will do the same for other jurisdictions.

In the eyes of many professionals, too many online businesses still haven't done enough to tighten security, enable more opt-in choices and assuage the fears of users who rely on their services to buy things, connect with friends and family, and post videos of their vacations. Users like you and me simply don't trust that these networks will completely protect their personal information from hackers and from other retailers who want in on all that user data.

So how much actual advancement has been made in the two years since the GDPR went into effect? *eWEEK* asked a large number of professionals the following question; their answers follow.

Q: What is the single most important aspect of the GDPR that is making (or breaking) commerce on the internet in 2020?

--

Tom Conklin, Chief Information Security Officer, Fivetran (https://Fivetran.com):

"Internet commerce has seen a spike in fraud this year. Many factors contribute to this and the GDPR is likely one of them. The GDPR's privacy rights can be exploited by malicious actors to hamper detection. This is not just on the e-commerce buyer side, but also sellers on e-commerce marketplaces can leverage anonymity provided by the GDPR to abuse platforms. This puts marketplaces within the E.U. at a disadvantage. An example is Amazon started doing video screening of third-party sellers in the U.S., U.K., China and Japan, and the E.U. is not included on this list. To combat this, companies are looking for ways to gain faster access to data to gain insights and detect anomalies as early as possible."

Joe Garber, Vice-President, Micro Focus (https://microfocus.com):

"The single-biggest factor to impact business in 2020 is the global spread of COVID-19, which is affecting how and where we work, and how we buy. Despite this new reality, the EU warned in March that GDPR still applies (https://www.europeandataportal.eu/en/news/gdpr-also-applies-during-covid-19-pandemic).

"While the conventional wisdom is that GDPR and related privacy regulations around the world are good for business (e.g., consumers have greater confidence in providing sensitive information, organizations have a framework for appropriately leveraging information to make more informed business decisions) some short-term challenges to commerce are being triggered.

"From a corporate perspective, the biggest challenge being presented by GDPR in today's environment can be found on the security front. *As more employees are asked to work remotely – in many cases an increase of 3X or 4X from just a few months prior – and as IT is being asked to scale to meet unprecedented demand, new vulnerabilities are emerging that can compromise privacy.* Organizations must therefore diagnose and address these new threats to identities, applications, and data in real-time, all while resources are being thinly stretched and often working in unfamiliar surroundings. Specific areas of concern include data on non-corporate owned devices as workers are having to use their personal equipment, and companies moving data to the cloud that must maintain secure as they do so.

"Organizations that have been most successful in pivoting to the post-pandemic business reality have been those that had already begun to digitally transform before 2020. For instance, an Austrian engineering company (https://www.microfocus.com/media/case-study/fcp-fritsch-chiari-and-partner-zt-gmbh-cs.pdf) recently reported that they were able to move 95 percent of their staff to a remote working setting within mere minutes. They comfortably adapted, while adhering to GDPR requirements, in part because they had prioritized digital transformation in advance.

"Obviously it's difficult to say how long this anomaly will last, or if some of the developing changes to commerce will be permanent. However, it's safe to say that digitally transforming – often with technologies underpinned by AI/machine learning that would help them scale and predict unanticipated risks – will be an important path forward to help organizations adapt to new realities while staying true to privacy requirements."

Stephen Manley, Chief Technologist of Druva (https://Druva.com):

"The storage limitation component of the GDPR has enabled e-commerce vendors to survive and even expand during this pandemic. To comply with the storage limitations, organizations defined and implemented data governance and data retention policies. Most organizations then implemented their policies using cloud--for protection of cloud and SaaS workloads, to meet data locality requirements and to handle their endpoints. When the pandemic forced the shift to a remote workforce, the well-defined approach to managing data has enabled their workers to maintain productivity without risking compliance violations. The use of cloud means they have been able to expand their businesses and tools without compromising their GDPR compliance. Storage limitation was the forcing function to create and implement policies that have helped e-commerce thrive in 2020. Of course, it's not too late for other companies to start taking those steps, even today."

Beth O'Callahan, NetApp (https://NetApp.com) VP of Corporate Legal and Chief Privacy Officer:

"The single most important aspect of the GDPR is how it became a catalyst for change in the industry: GDPR didn't just change privacy policy disclosures, it changed how companies think about their data needs, monetization strategies, and growth plans. Furthermore, it drove changes not only to the ways, types, and amounts of information companies shared, but also created new business incentives and competitive advantages for companies who invest in privacy technology. As more data is moved to the cloud, GDPR is driving trust in companies—including cloud service providers—with the management of data, including customers' personal information. GDPR provides a framework on which companies can build programs to earn customers' trust, as it provides the structure for candid conversations about the collection, use, and sharing of personal information."

Rob Parrish, Senior Director, Product Management, Arm Treasure Data (https://www.treasuredata.com):

"The single most important aspect of the GDPR for eCommerce is consent conditioning specified in Article 7. New innovators must leverage consent as part of their consumer engagement strategies, by building trust through every stage in the customer data journey. The rise of awareness of a customer's privacy and the sense of ownership are shifting their buying decisions for more privacy-friendly services. Companies that have a strong understanding of their customer data for engaging experiences and demonstrate their privacy practices, are winning the trust of their customers and successfully scaling their businesses."

Barbara Lawler (https://www.linkedin.com/in/barbaraklawler), Chief Privacy and Data Ethics Officer at Looker (https://looker.com):

"The EU General Data Protection Regulation (GDPR) has been one of the most defining pieces of IT regulation for businesses and society, in recent years. May 25, 2018 marked the start of a journey toward data compliance, governance, privacy and security for many companies, and this process is far from over. While these topics are without a doubt top of mind for anyone working with data, many companies are still struggling to reach the required level of compliance and governance. But companies shouldn't view GDPR as a challenge, but rather as an opportunity to get a better handle on their data.

"Below a are a few things that those companies with a thoughtful data-driven culture have probably done to reach GDPR compliance within the first year:

- **Centralize data.** Most companies today rely on a multitude of cloud services and applications which all require access to real-time data. Businesses who have a single access point for their data have it so much easier to oversee all activity and therefore analyze it and find potential GDPR breaches in a fast and effective manner.
- **Monitoring & Auditing.** Of course companies have been checked regarding their GDPR compliance status – and will continue to be checked. In order to be able to remain compliant, businesses have to make sure to conduct regular audits of their own privacy protection practices and keep records of all data that is held, processed and transferred.
- **Appointment of a DPO.** According to the GDPR regulation, companies whose core activity involves extensive processing of personal data must appoint a data protection officer (DPO). The DPO is responsible for monitoring all data subjects and must conduct regular audits to ensure compliance and address potential privacy issues.
- **Confirm legal basis to process data**. Transparency and ensuring that consumers have control over their data is at the core of GDPR. Thus, companies have to make sure to determine in advance the purposes for collecting and storing data, whether through customer consent, fulfillment of a contract, legitimate interests, or other basis. In the end, users' rights are overriding the rights of the data controller, so they must be able to request access to, correction of, restrict usage or the erasure of their data.

"Companies that implement these structures and policies can create a thoughtful data-driven culture, which is the very basis for GDPR compliance. Once data enablement has been established, companies will not only profit from being GDPR-compliant – as opposed to some competitors – but also from the valuable insights that their centralized data offers them."

Andy Teichholz, global industry strategist of compliance and legal at OpenText: (https://OpenText.com)

"GDPR provisions around subject rights have had dramatic impacts for online business. First, the increased consent and opt-in standards mean that marketing lists have been decimated. As many as 50+% of businesses marketing contacts have opted out. While this means a smaller audience, the silver lining is that the consenting audience is more engaged. Additionally, not only are businesses worried about losing some of its sale channel due to these standards, but they are also concerned about customer retention and brand loyalty. Other GDPR challenges, such as the inability of businesses to adequately or timely respond to Data Subject Access Requests (DSARs), have the potential to further erode customer loyalty, retention, and trust beyond the non-compliance risks and operational burdens they also face."

Ameesh Divatia, co-founder and CEO of data protection provider Baffle (https://baffle.io):

"It's about data privacy/using data responsibly. GDPR was hailed as 'the most important change in data privacy regulation in two decades.' And it was the first real security regulation with significant teeth. Originating in the EU, GDPR empowered consumers to not only have a right to know what their data will be used for, so the data collectors have to provide purpose, but they also have the right to be forgotten.

"Data is the new oil, where you can get so much value out of it. But it is also the new asbestos, which means that if companies don't use the data responsibly, the consequences can be devastating. We want to create solutions where this unethical behavior is not only prevented, it's actually mathematically impossible because of the safeguards we have designed and can put in place where no data is provided in the clear, even while it's being processed.

"In response to GDPR, CCPA and other regulations in force or currently being considered, we have developed the mechanisms to process the data, without compromising privacy. With GDPR in play, the motivations of companies needed to shift from compliance and defending against litigation and fines to a relationship of trust. This means treating customer information not as a currency or commodity but instead as the most valuable bond between a company and its users and customers. As a result, companies are starting to learn that security is a competitive differentiator, which is a positive for building trust, and not a necessary evil that is a checkbox for compliance."

Nigel Tozer (https://www.linkedin.com/in/nigel-tozer-329763/?originalSubdomain=uk),Commvault (https://www.commvault.com/) Director, Solutions Marketing, EMEA:

“GDPR has certainly exposed the issue of trust. Who can we trust with our data? Does every modern business want to turn us into a data product? The way cookie walls are configured and the language used in privacy policies expose the intent of the organization behind them. Being compliant with GDPR (or CCPA) doesn’t automatically make your business trustworthy, of course, but it gives us many clues to ones that are – and trust will be a critical success factor for many businesses coming out of the current situation.”

Gerald Beuchelt, CISO, LogMeIn (https://LogMeIn.com):

“GDPR has created a heightened sensibility for privacy and security both with consumers and businesses. Businesses had to invest deeply in new processes and technologies to comply. Enhanced compliance monitoring will put additional stress on small and medium businesses, who are already suffering from COVID-19 shutdown losses. Regulators will need to apply restraint to not use GDPR in a way that is even more harmful to the economy. At the same time, it will be interesting to see if governmental agencies are compliant with privacy requirements, especially in the light of demands for population health surveillance. GDPR and related privacy regulations will lose a lot of credibility if governments can simply exempt themselves from these regulations.”

Nigel Hawthorn: McAfee (https://mcafee.com) Data Privacy & Cloud Spokesman, EMEA:

“The two years since GDPR was introduced seem to have been awash with data loss incidents and through this time consumers’ understanding of the value of their personal data has increased. It has made retailers be more proactive in data minimisation, security and control; with the threat of bad publicity, losing customers and remedial clean-up costs being of greater concern than the individual fines. The areas that we see are still misunderstood is that data controllers are responsible for all actions of any third-party processors – I believe the next wave of actions will be corporations taking a tougher line on their subcontractors, outsourcers and cloud providers.”

Nick Emanuel, Senior Director of Product, Webroot (https://Webroot.com), an OpenText company:

“The value of data has never been more apparent. In the two years since the GDPR came into effect, there has been a significant shift in the way that data is regarded, utilized and protected. Its value has been particularly apparent recently with several high-profile data breaches, highlighting that even companies who are regularly trusted with sensitive personal data can be successful targets for cyberattacks. We’ve also witnessed cybercriminals demanding even higher ransoms for stolen data.

“As high-profile leaks and breaches continue to make the news, we’re likely to see authorities across the EU get tougher on GDPR violations and data breaches in the coming year. The penalties are real and they are significant. This means companies need to take recent cases as a wake-up call to address their data security and privacy compliance quickly if they are not already. From a reputation protection standpoint, being in the spotlight for data protection transgressions and data breaches is not at all good for business.

“Pressure will mount on business leaders to take action to cut costs and security spend may be highlighted for reduction. However, the economics here are clear – cybercriminals are not cutting their budgets and are waiting to exploit weaknesses. With the unprecedented shift from office to W.F.A (Working From Anywhere) it’s crucial that businesses review their remote working policies for data protection as well as security and be prepared for the variety of different work environments."

Peter Gregory, senior manager, risk advisory at Optiv Security (http://www.optiv.com/):

“The critical issue for e-commerce is this: Organizations are doubly responsible for protecting the personal information that they decide to keep on file for all of their customers. Plus, organizations have been forced to switch their business models from “opt out,” to “opt in.” This means that they must be transparent about how they will use that data: They can’t simply do whatever they feel like (selling to others, telemarketing, etc.), as in the past, unless they are explicit about that in their privacy policy. Further, they are required to set up business processes whereby their customers can contact them to ask to see their data, to understand how it’s used, and to remove it altogether.”

Steve Wood, CPO of data integrator Boomi (https://boomi.com):

"The introduction of GDPR led organizations to adopt solid data strategies, which included previously overlooked metadata. If there’s no metadata management, you can’t have compliance. Without it, businesses can’t have an accurate picture of the data in their possession, what it represents, its origins, its current location or its iterations, or even who can access it, and therefore cannot fulfill their accountability obligations.

"Under the GDPR umbrella, correct metadata governance sets the foundation for compliance, as it brings transparency to the information supply chain and assigns accountability and control as necessary.

"The ability to make decisions for the business based on the correct insights while avoiding the pitfalls of tightening regulations has never been more critical. Visibility into metadata helps ensure companies meet GDPR’s requirements for the right to access and the right to be forgotten. Those who implement thorough metadata management systems will find themselves ahead in the race to survive and thrive in today’s crowded competitive landscape."

Terry Ray, (https://www.linkedin.com/in/terry-ray/) SVP and Fellow at cybersecurity provider Imperva (https://www.imperva.com/company/about/):

"A year before and a year after GDPR began, businesses raced to meet as many of the GDPR directives as possible. Meeting them all is a large ask for most organizations and the larger the organization, the more complicated the work is."

"Like most regulations, GDPR provided a somewhat lenient grace period to give a little more time for compliance, but as we complete year two, the expectation now that companies will comply are doing so (and those that have chosen not to), are not as a choice. This could be as a result of companies growing, acquisitions, moving to cloud, and shifting from internally managed data to outsourced."

"The transformation of IT in companies is never-ending and so is the effort to track, classify, audit and protect private data. I categorize the first two years as the sprint and the rest as the never-ending marathon. The sprint is over and now begins the marathon."

"GDPR has taken some of the priority that existed for regulations like PCI, SOX, local privacy laws and others, and focused it on consumer privacy with highly visible requirements so we all know companies appear to be protecting our data. An obvious example being our need to always click 'accept' for cookies on every website we visit now."

"Does this mean that the business is doing the right things to protect data? Still today, most businesses, particularly large ones, still do not know where all private data is located, who has access to it, and who actually uses that access. Much less can they actually tell the last time someone accessed your data or how much data was actually accessed. Most businesses today monitor access to less than 10% of their data and focus their monitoring on privileged human users, which make up a very, very small amount of the transactions on data. They ignore the rest, which does not sound secure and responsible."

"Ultimately, this means that even with regulations, businesses fail to have appropriate knowledge about their most critical asset, which for GDPR purposes, may also be your most critical asset – everything about you."

Lisa Plaggemier, Chief Strategy Officer of cybersecurity and privacy education firm MediaPRO (http://www.mediapro.com):

"How it (GDPR) impacted the IT side was that it forced a lot of projects to the forefront that needed doing but didn't have support before the regulation. The issue of personally Identifiable Information (PII) and Sensitive Personal Information (SPI) is a perfect example. Without visibility into where this information was, exactly how much a company holds, where it was being stored, how it was being transmitted, stored and disposed of, the security team couldn't protect it. The GDPR put wind in those sails. Funding support for a large-scale data discovery project became available solely because of the (then-new) regulation."

Camilla Gjetvik, Chief Operating Officer for Norway-based boost.ai (https://boost.ai):

"There is no doubt that the implementation of the GDPR has impacted and influenced our business. The free flow of information has been instrumental in helping the internet to grow into an invaluable tool, and that the flow needed to be regulated in a more stringent way to address concerns about ownership and transparency.

"For us the implementation of the GDPR did not only raise compliance questions, it has also been the catalyst for many ethical questions and discussions that both, we as a trusted company; but also our customers should be asking regarding the collection of personal data.

"For us, it was interesting to challenge ourselves on how much real data we would actually need to build our AI models. In fact, we asked ourselves how much we could minimize the necessity to collect data from customers. Interestingly, we found that no actual or real customer data is required to train our model for it to grow and improve.

"This gave us a competitive edge, which I believe differentiates us from many other companies, who are more focused on how much data they can collect and monetize. GDPR allows boost.ai to compete in the global marketplace and help to create a world of ethical, trustworthy AI."

Raghu Nandakumara, Field CTO in EMEA and APAC at Illumio (https://www.illumio.com/%20%E2%80%8E%20%E2%80%8E):

"If you were to summarize GDPR into a single sentence, it is about ensuring that the subject of personal data has much better control over and transparency into the use of that data. This is a significant shift from previous approaches to personal data protection, where it was either an all or nothing scenario – the subject could grant access to their personal data and, while benefiting from how it was leveraged, also have no control over the myriad of other ways in which it was being utilized, shared, and maintained; or they could not provide any access and have to find other, less accessible, methods through which to realize the benefits, if at all.

"GDPR has pushed organizations to adopt much better technology practices. Now, from the start of a project, organizations make decisions with data privacy requirements top of mind – that's a huge shift from the approach we saw even three years ago. There's no denying GDPR's impact on enterprises.

"In a typical enterprise one of the focus areas for information protection is the network. The corporate network is assumed to be trusted and therefore, by default, everything on that network is also deemed to be trusted. What's interesting is that when we think about network security, we could say that the old approaches to data protection were like being on an implicitly trusted network – once you attached your device to that trusted network, you worked under the assumption that everything else on the network was also trusted and acting in good faith, akin to granting a third party access to data and assuming that all future use of that data is for legitimate, authorized reasons.

"Contrast that with a Zero Trust approach to security which enterprises are beginning to adopt. Here each actor – whether it's an individual, device, network, application, or data – has a well-defined, explicit, always monitored set of actions and privileges that they can perform, and these are limited to the smallest set they need to perform their job. This approach to security not only maintains least privilege, but taking a "User A can only do X or Device B can only access Y" approach to defining policy leaves no ambiguity into the overall security posture of the environment since it is simply a union of all of these conditions.

“GDPR, in essence, is taking a similar approach with data protection in that it ensures that there is far less ambiguity with what the data is, who has access to it, how it’s being accessed and used, and that the data is always in a correct state. In short, clarity is on the rise, both in cybersecurity and data protection.”

Aaron Shum, security, risk and compliance lead analyst at Info-Tech Research Group (https://www.infotech.com/):

"Recent insights from GDPR enforcement statistics (https://can01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.enforcementtracker.com%2F%3Finsights&data=02%7C01%7Cirayghosal%40infotech.com%7Ceea221cedc1a43ed34bd08d7fe4da14 show that GDPR enforcement actions have dropped significantly in light of the ongoing COVID-19 crisis. However, the pandemic does not mean there is a moratorium on GDPR compliance. Businesses are inadvertently aggregating exceptional information in order to deal with pandemic response, including additional health related information of their employees and employee family members. It will be crucial for businesses to track/tag pandemic-related data separately to ensure compliance, and set very specific retention windows so the data can be purged as soon as it’s no longer necessary, especially due to the sensitivity of contact-tracing.

"GDPR has forced many large scale application providers to build privacy controls into their platforms, due to the Privacy by Design requirement within Article 25 of GDPR. However, many organizations initially reacted to GDPR by doing the bare minimum, putting up generic privacy policies and cookie consent walls as a means to show they have “done something.” The advent of remote work brought on by COVID-19 exposed many instances where the impacts of GDPR have yet to take place, as was the case with the recent scandal with Zoom security and privacy. Smaller application providers will often do “just enough” to satisfy the risk-based approach to GDPR advocated by the European Data Protection Board (the governing body for GDPR), leaving these platforms vulnerable to security and/or privacy exploits when data volume scales up; the larger the sample, the larger the exposure."

Brenda Ferraro, VP of Third-Party Risk for Prevalent, Inc. (https://www.prevalent.net) and former CISO for Aetna:

“Over the past two years, GDPR brought the need to create more robust Data Protection Authorities (DPAs) and Data Protection Officers (DPOs). The focus on digital transformation of public and private sector data protection forced businesses to dive into their financial pockets to instill global data compliance all the way from onboarding, to processing, to offboarding their third party engagements.

“Coming upon the second year anniversary of GDPR, it is important to recognize that the ‘mine, mine, mine’ aspect of the regulatory requirement has potentially saved the globe from increased vulnerability and exposure during our current crisis due to the heightened GDPR due diligence. However, GDPR continues to be a work in progress and many companies have taken a pendulum swing towards strict interpretations of the framework causing scarcity of data driven decisions along with suppressing innovation causing information overload and caution to push aside relevant due diligence and data usage.

“For third-party risk management, where more than one company is processing activities, this year will need to place a new focus on how to effectively ensure compliance where control is shared amongst more than one company. Let us not forget the drive towards AI, additional laser focus will need to be specific to enabling fit for purpose right-sized data protection impact assessments. All in all, it has been 2 GDPR years well spent with definite room for improvements to make it easier with clarity.”

Danny Allan, CTO of Veeam (https://www.veeam.com/):

“It’s been two years since the European Commission (EC) made its highly anticipated General Data Protection Regulation (GDPR) enforceable on May 25, 2018. The regulation, which replaced its predecessor, the Data Protection Directive from 1995, continues to display two key characteristics: it’s both specific, and it has teeth.

“The impact of these characteristics has resulted in data privacy becoming globally recognized globally by IT businesses and leaders. As a result, other countries have started to develop and implement their own privacy laws. Earlier this year, we saw the California Consumer Privacy Act (CCPA) – the US’s first data privacy law – go into effect. This movement to implement new laws can be viewed as forward momentum and a success for the technology industry and for IT businesses. Technology is unable to reach its full potential until consumers have the trust required in the security and privacy associated with their data.

“Since GDPR was introduced two years ago, IT businesses have started to recognize that data collected today can be mined for insight tomorrow. For example, it can be used to create better user experiences, develop products which address genuine market needs, and reward customers for loyalty. As user awareness increases, tolerance towards organizations who are seen to be collecting, but not respecting data, will get lower. Therefore, organizations that fail to get to grips with data privacy, making privacy part of its corporate culture, will face a backlash from customers, as well as draconian punishments from regulators. Data privacy and protection should not be viewed as a box-ticking exercise, or something you just do because you must.

“Looking ahead, public awareness of, and demand for, stronger data protection practices are likely to continue to increase, especially as more security breaches and privacy concerns continue to make headlines. Privacy will evolve from a European-based GDPR discussion to a more global compliance initiative with organizations struggling to provide users with some control and visibility over their data.

Dianne Lapierre, CIO at Absolute Software (https://www.absolute.com/):

“Since its inception, GDPR has guided organizations of all shapes and sizes in establishing stricter privacy policies. However, what’s interesting is that this pandemic is exposing how it may not be being followed as strictly as most might think. Absolute recently published an Remote Work & Distance Learning Insights Center for Enterprises and Educational Institutions to be able to manage, monitor and measure their WFH and LFH initiatives against millions of Absolute’s 8.5 million activations as a benchmark. The data, being updated weekly, is astonishing:

- **Sensitive data is piling up on enterprise devices.** There has been a 43 percent increase in the number of items of sensitive data - such as Personally Identifiable Information (PII) and Protected Health Information (PHI) - identified on enterprise endpoints, compared to pre-COVID-19. Compounded by the pre-existing gaps in endpoint security and health, this means enterprise organizations are at heightened risk.

- **Enterprise organizations are at heightened risk of breaches or compliance violations.** On average, one in four enterprise endpoint devices has a critical security application (Anti-Malware, Encryption, VPN, or Client Management) that is missing, inactive, or out-of-date. With the significant increases in sensitive data being stored on these endpoints, enterprises are putting themselves at risk of legal compliance violations and data breaches as COVID-19 cyberattacks accelerate."

Garth Landers, Director of Product Marketing, Mimecast (https://www.mimecast.com/):

"Much of the public attention on GDPR has been focused on the lack of fines levied at big tech firms and a collective feeling that maybe this doesn't matter as much as suspected. For businesses, this is the farthest thing from the truth. The need to know what data you have, understand the rationale for retaining it and identify how quickly you can retain it has had an incredible impact. Many businesses had really under invested in information management goal setting in the past. GDPR changed that.

"Enormous investments in personnel, technologies and processes focused on data privacy have become foundational in many organizations impacted by GDPR. Many investments in technology come with a need to assess the impact on GDPR now. For example, moving to the cloud or hosting an on-premise database that may contain customer data require a GDPR impact assessment. In higher education, records from personnel or students – in many cases very old data – have merited GDPR impact consideration, based on Mimecast customer experience. So, the impact of GDPR is constantly evolving. GDPR is not a one-time event. It's a continuous state of business, so all of these things – people, technology, audit processes etc. – are still ongoing.

"We are still at the early stages of fully understanding the GDPR impact. It's going to live on (like most regulations) and today we see more regionalized similar privacy regulations such as CCPA emerging across the globe. As a result, multinational organizations and others will have to amplify their efforts. The good news is that early investment in GDPR readiness will pay dividends as the regulatory landscape evolves.

Tim Mackey, Principal Security Strategist, Synopsys (https://www.synopsys.com/) CyRC:

"With the second anniversary of GDPR approaching it's time for us to go on the offensive and hold the people collecting data on us more accountable Regulations like GDPR provide individuals the ability to request what data a company already has collected, but the fight to control data actually starts with its collection and not reviewing what is already out in the wild. I submit that if more people asked their vendors or providers of services they're subscribed to what data they collect, how its secured, how long its retained for, precisely who its shared with, who has access to it and under what conditions, and how they would detect that someone accessed your data without proper authorization – then we'd start having consumers driving the agenda for data protection rather than being passive recipients of breach notifications containing offers of credit monitoring. Even if the answer is a highly technical one that might not be immediately understandable, the act of asking sends a signal that the consumer cares about how their data is used and managed.

"Of course, on the business side, if the vendor simply cites their license agreement or privacy policy, then that vendor is in essence saying one of two things. The first, and likely most common, is that their license agreements and privacy policies are written in generic terms. In this situation as the application and services they provide evolve, the use of generic terms helps ensure that developers don't need to have a legal review of any changes because the agreement is so vague. The second, and least likely scenario, is that the company has developed a constructive partnership between their development teams and their legal counsel.

"Under such a model, the policies can accurately reflect the current state of what data is being collected, processed and retained by the vendor. As users, the only way to detect which situation is real is if the answer to your questions simply point to a license agreement or privacy policy, then ask when that document was last updated and what version of their software it covers. If the software is newer than the last review, the policies are generic. Importantly, the act of asking these questions will cause the customer support team to log your request and how it was answered. While the initial response might be less than helpful, with more customers asking for the same information, the business will eventually recognize that their customers and prospects value clear and accurate disclosures of what data is collected, how data is being processed and expect to be active participants in understanding how their data is used."

Rajesh Ganesan, VP, ManageEngine (https://www.manageengine.com/):

"Privacy laws will result in increased focus on employee accountability. More countries are following the European Union's lead by implementing data protection laws similar to GDPR, such as the Thailand Personal Data Protection Act (PDPA) which goes into effect in this month. Under such scenarios, the role of Data Protection Officers (DPOs) assumes significance as they must work closely with the CIOs and tech teams to ensure that organizations comply with the law. With increased awareness of and emphasis on data protection, there will be an even greater focus on the handling of users' personal data and its security. Employees at all levels will be held accountable as organizations strive to meet compliance. Therefore, there will be a need for upskilling and education programs to handle this aspect.

"This is also the right time to take security very seriously. In the wake of this pandemic, it is easy to bypass all your processes. Build it from the ground up; the last two years were wonderful. GDPR coming from the European Union was a game-changer, but we need to make sure we continue to address security and privacy at the foundation level."

Kon Leong, CEO and co-founder, ZL Technologies: (https://www.zlti.com/)

"Even two years after its enactment, companies have insufficient technology to meet GDPR. Regulators have barely begun to scratch the surface of the problem, and do not yet understand the digital ecosystem enough to properly address fines. The lack of significant fines under GDPR can be attributed to the fact regulators have come face to face with the complexity of implementing data privacy in large enterprises, and the reality that we are still years away from being there."

Guy Cohen, Head of Policy, Privitar (https://www.privitar.com/):

“The last two years have seen privacy become a boardroom issue. This has partly been due to the GDPR, but also because of the wider social change to prioritise and expect privacy following various data breaches and scandals. GDPR has been the regulatory expression of this in Europe, but it's also been seen in customer expectations and the emergence of privacy as a competitive differentiator. The GDPR's focus on accountability has required a shift in business culture, to a new focus on demonstrable compliance. The possibility of high fines and losing customer trust has boosted demand for privacy technology solutions, and the last two years has seen a range of new tools mature and organisations build or expand internal privacy and data governance capabilities.

Privacy as a core requirement is here to stay. The GDPR was an evolution of the 1995 Directive, it's not the start of data protection law, and it won't be the end. In the coming years with new regulatory opinions and case law we expect privacy best practices to become clearer and raised over time. Meanwhile the GDPR is already influencing a wave of new privacy legislation around the world, becoming a new global standard. We expect the business practices and technology needs it led to to follow."

Gil Cohen, General Manager of the Multi-Channel Recording and Voice Biometric LOB, NICE (https://www.nice.com/):

“Two years ago, the EU General Data Protection Regulation (GDPR) completely changed how organizations, across every sector and industry, practiced and viewed compliance. The current pandemic has highlighted that it’s more critical than ever for organizations to approach compliance with a careful, strategic eye. The high importance placed on consumer privacy will only continue to fuel changes in the modern enterprise – shaping new technologies, processes and strategic leadership to guide initiatives.

"With the onslaught of CDPA and CCPA legislations, and the responsibility to protect consumer data at an all-time high, it is essential for brands to activate transparent, efficient compliance efforts. Compliance capabilities powered by AI-driven analytics and automation play an important role in enabling this. Ultimately, brands need to view privacy as a competitive differentiator when it comes to fostering trust, and fulfilling the promise of better customer experience and executing to ensure brand loyalty.”

George Gerchow, chief security officer, Sumo Logic (http://sumologic.com):

“We will see a movement emerge in the tech industry to streamline privacy. As we approach the second anniversary of GDPR, the industry has continued to see data privacy regulations come to the forefront of business conversations around the globe, both at the national and local levels. Earlier this year (Jan. 2020), the California Consumer Privacy Act (CCPA) also went into effect within the United States - a bill similar to that of GDPR that impacts not only the local region but also all U.S. and foreign entities that conduct business with the state of California. Many of these regulatory acts outline robust data protections, but they lack a clear path to implementation. To avoid disruption to business and day-to-day operations, we’ll see increasing demand for the tech industry to come together to streamline privacy and adopt a consumer privacy-by-design mindset.

Rhushabh Mehta, SVP of Engineering and R&D, White Ops: (https://www.whiteops.com/)

“GDPR and CCPA are a good start to the problem of ensuring people's privacy; but both guidelines put too many requirements on the customer to initiate a set of actions to protect themselves. Companies will invest a lot of money and time to comply with these policies to be "good enough," but, it does not reach the root of the problem – to be foundationally privacy-conscious. For example, the debates we are having now about cookieless environments are going to force us to choose between service and privacy. That seems awkward, if privacy was part of everyone's core philosophy and every company protected data as if it were weaponizable; we would not have to choose. For example, IP Addresses could be used to deliver location-specific ads at the moment but that are only stored in an obfuscated manner using one of the many privacy-centric algorithms. This way, even if someone else managed to get a hold of the data it would be useless. Privacy needs to be about fundamentals - not just controls and processes.”

Jennifer Marcus, General Counsel, White Ops (https://www.whiteops.com/):

“Two years later and the privacy landscape is still somewhat murky when it comes to GDPR. This previously dreaded 4-letter acronym has become the impetus for a multitude of other privacy and data-protection legislations, but was its bark bigger than its bite? What was purported to increase transparency and accountability for companies processing large amounts of data remains to be seen. Even though companies now have to provide justifications for their data processing, usage, storage and any grounds for exemptions, the guidelines of GDPR are still unclear and industry-wide compliance seems dubious. GDPR is more interested in fining large internet platforms and walled gardens as opposed to creating clear guidelines for implementation, resulting in companies being fearful of those steep fines and overly notifying the EU data protection authorities. This lack of clear guidelines and multiple interpretations of the present legislation, coupled with the already-inundated EU data protection authorities, has resulted in confusion and lack of protocol. The legislation is certainly imperfect, but the industry is hopefully improving.”

John Samuel, Executive Vice President, CGS (https://www.cgsinc.com/en):

“According to a recentsurvey (https://www.cgsinc.com/en/resources/customer-service-in-crisis), concern about data safety increases as consumers age. Americans over-65 were the least confident (41%) in how their data is being used by companies, while younger consumers continue to be more willing to share information to enjoy the personalization and ease of digital interactions. They are savvy and comfortable with technology, as having grown up with it, and know how to use privacy settings to monitor or block tracking which makes them more comfortable weighing convenience over privacy.

“Overall, it’s clear that further education is needed to help users – especially the over-65 group who are not as comfortable with technology – feel more secure with how their personal information is used and protected. They need to understand what privacy controls currently exist to keep them safe and beyond this, they need more insight into how they can be their own best protector of sensitive information and how they can navigate the controls. At the second anniversary of GDPR, there is no better time to apprise the public that any company doing business in the European Union, including U.S.-based multinational organizations, must be in compliance with GDPR, privacy and all the controls available to the users.

“As consumers continue to be anxious about the security of their data, now is the time to provide them the information and control they need to feel confident that their data is safe. For companies that haven’t refreshed or restated their privacy policies since GDPR first went into effect, reviewing and updating, as necessary, these policies should be a priority – it will be critical to retain customers and differentiate platforms with a focus on privacy controls.”

Grant Geyer (https://www.linkedin.com/in/grantgeyer/), Chief Product Officer at Claroty: (https://www.claroty.com/)

“Just as important as the principles the regulation stands for, the European Union’s global enforcement of blatant and willful violations of the rights of European citizens to have their personal data safeguarded has raised its prominence to the gold standard of data protection regulations worldwide. In today’s global economy, GDPR has swiftly created a replicable regulatory blueprint that represents a win for citizens to maintain ownership over their personal data. That’s a sacred right in a digital economy where for many years personal data has been abused and monetized without awareness, consent, or recourse.”

Vijayanta Gupta, vice president, product & industry marketing, Sitecore (https://www.sitecore.com/):

"Pre-GDPR, many brands’ personalization efforts were based primarily on influencing customer behavior vs. focusing on their needs through a customer-first mindset. For this, many brands used a catch-all approach of collecting all types of data, regardless of if they could use it to deliver value to the customer. I call it the 'wild west' of customer data collection, which was so easy to do with the help of technology. Technology that often did not have the right controls in place.

"The situation has now evolved. Brands are putting more effort toward planning and communicating their intended use of customer data so they can execute well-planned content personalization initiatives with a customer-first mentality. However, this is just the beginning. Brand communication and user awareness both need to evolve further as digital engagement goes beyond the screen and permeates everything we do, especially with the emergence of 5G and the evolution of the Internet of Things."

Buno Pati, Infoworks (https://www.infoworks.io/) CEO:

"Monday marks the second anniversary of GDPR, and it also marks the tip of the iceberg with regards to the protection and consumer control of consumer data. As a global society, we need to trust our privacy is safeguarded. Throughout 2020 and into 2021, consumer control of personal data can be expected to increase dramatically as governments and regulators drive new privacy legislation. Within a decade, these regulatory actions will likely lead to complete consumer control of personal data and opportunities for consumers to directly monetize their data or directly exchange data for goods and services."

Sovan Bin, CEO of Odaseva (http://www.odaseva.com):

"As new technologies enable the collection of greater amounts of data online, it is essential that organizations consider privacy at every stage of their operations–shifting the burden away from consumers, who even today shoulder the responsibility to understand their rights to privacy. And the challenge of ensuring data privacy has become even more pressing: organizational boundaries are no longer static, making it difficult to track how, where, and by whom information is being stored, managed, and accessed. This is the time for a quantum leap in data privacy protection.

"Privacy by design that is a framework for proactively embedding privacy into the design and operation of IT systems, business processes, networked infrastructure, and business practices. It’s designed to protect consumer’s data, but it dictates and provides a guideline for how organizations must handle consumer data."

Juan-Carlos Colosso, Director of Privacy Product Management, Adobe (https://Adobe.com):

"Two years ago, GDPR transformed the way many think about privacy, sparking legislative and regulatory activity globally, inspiring new laws like the California Consumer Privacy Act (CCPA) and the Brazilian General Data Protection Law (LGPD). It’s clear the regulatory landscape is ever-evolving and there’s no one-and-done approach, making the partnership between IT and privacy teams imperative. A successful partnership requires IT and privacy teams to openly communicate and collaborate with not only each other but also the broader organization, creating forums for discussion that increases influence across products and services to strengthen company-wide alignment.

"Together, the two teams can establish a strong foundation of privacy by design that will help enable the organization to successfully navigate the privacy landscape – building enjoyable, transparent user experiences that inherently prioritize privacy and in turn, establish trust and loyalty with their audience."

Bob Swanson, Security Research Consultant, Swimlane

"Although this isn't a primary intent, GDPR continues to influence how businesses approach and interact with personally identifiable data (PII). Like any legislation in its infancy, specifically an evolving concept like data privacy, there will have to be ongoing improvements and feedback from various parties involved in the process. One area needing clarification and that many organizations are turning over in their heads is what actually constitutes consent. Similar gray areas of the legislation will force authorities and businesses to come together in hopes of establishing clearer, more well defined interpretations of the law."

Sponsored Content (https://www.datamation.com/cloud-computing/slideshows/10-leading-artificial-intelligence-companies.html?utm_source=quinstreet&utm_medium=native&utm_campaign=housebanners01162020) on eWEEK

10 Leading AI Companies (https://www.datamation.com/cloud-computing/slideshows/10-leading-artificial-intelligence-companies.html?utm_source=quinstreet&utm_medium=native&utm_campaign=housebanners01162020)

By Datamation (https://www.datamation.com/cloud-computing/slideshows/10-leading-artificial-intelligence-companies.html?utm_source=quinstreet&utm_medium=native&utm_campaign=housebanners01162020)

(https://www.datamation.com/cloud-computing/slideshows/10-leading-artificial-intelligence-companies.html?utm_source=quinstreet&utm_medium=native&utm_campaign=housebanners01162020)

Sponsored Content (http://www.eweek.com/SponsoredNews.php?prx_t=JdgFAeYtDA3iAQA&ntv_eg=3*303;&ntv_fr) on eWEEK

How Can 'Shifting Left' Transform Your Tech Support? (http://www.eweek.com/SponsoredNews.php?prx_t=JdgFAeYtDA3iAQA&ntv_eg=3*303;&ntv_fr)

By Rimini Street (http://www.eweek.com/SponsoredNews.php?prx_t=JdgFAeYtDA3iAQA&ntv_eg=3*303;&ntv_fr)

(http://www.eweek.com/SponsoredNews.php?prx_t=JdgFAeYtDA3iAQA&ntv_eg=3*303;&ntv_fr)

‹ (/security/ibm-think-2020-digital-building-reliability-resiliency-in-uncertain-times)

Previous
IBM Think 2020 Digital: Building Reliability, Resiliency... (/security/ibm-think-2020-digital-building-reliability-resiliency-in-uncertain-times)

Next
How Using AI Vastly Improves Threat Detection (/security/how-using-ai-vastly-improves-threat-detection)

› (/security/how-using-ai-vastly-improves-threat-detection)

Chris J. Preimesberger

Chris J. Preimesberger is Editor-in-Chief of eWEEK and responsible for all the publication's coverage. In his 15 years and more than 4,000 articles at eWEEK, he has distinguished himself in reporting...

View full bio › (/Authors/chris-preimesberger)

Research Assistant on eWEEK

Top IT resources to move your business forward

Which topic are you interested in?

Security

Networks/IoT

Cloud

Data Storage

Applications

Development

IT Management

Join the discussion!

Recommend Share **1 Comment**

WeCode Inc - 2 weeks ago

Keep up the great work. Thanks for the share

Reply

LoudVoice Comments **Privacy Policy** **Powered by OneAll**

(/)

Contact Us (/contact-us.html) | About eWeek (/about-us.html) | Sitemap (/sitemap.html)

(https://twitter.com/eWEEKNews) (http://www.facebook.com/pages/eWEEK/49650732622) (https://www.linkedin.com/company/eweek-washington-bureau?trk=company_name) (https://www.youtube.com/user/eweeknews)

Property of TechnologyAdvice.
Terms of Service (https://technologyadvice.com/terms-conditions/) | Privacy Notice (https://technologyadvice.com/privacy-policy/) | Advertise (https://technologyadvice.com/partners/) | California - Do Not Sell My Info (https://technologyadvice.com/privacy-policy/ccpa-opt-out-form)

Advertiser Disclosure: Some of the products that appear on this site are from companies from which TechnologyAdvice receives compensation. This compensation may impact how and where products appear on this site including, for example, the order in which they appear. TechnologyAdvice does not include all companies or all types of products available in the marketplace.