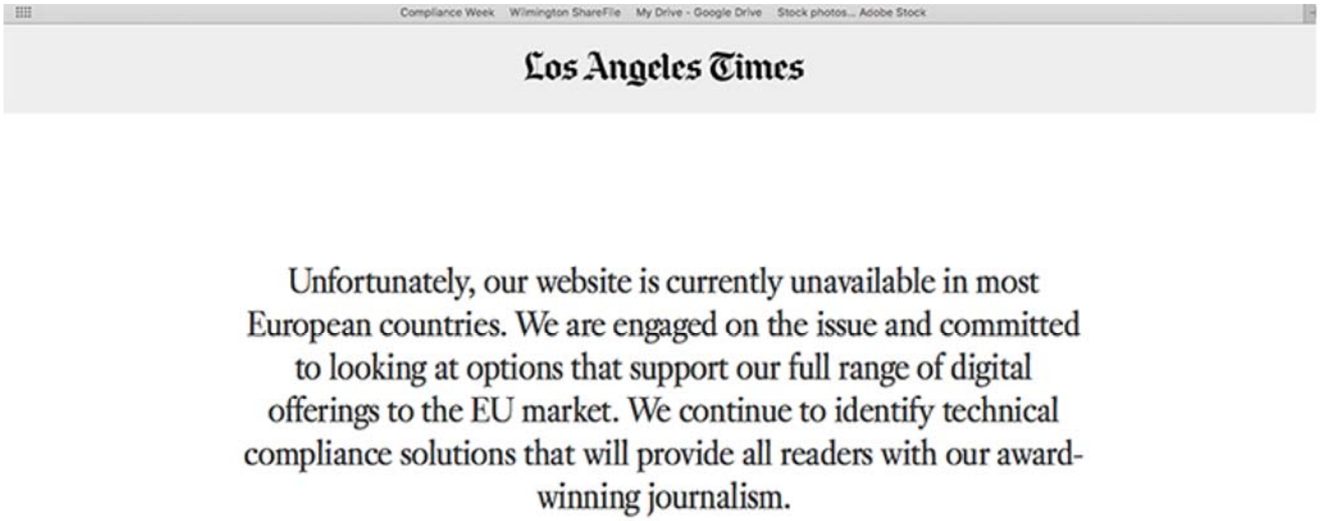
News



Taking a pull-the-plug approach to GDPR compliance

Neil Hodge | June 5, 2018

Given the two-year lead time, few would have guessed that the best way some organisations would comply with the European Union's stringent new data rules would be to simply cut access to services.

On 25 May, as the EU's General Data Protection Regulation (GDPR) came into force, dozens of Websites shut down their activities completely, while others forced users to agree to new terms of service—some by flooding inboxes with e-mails asking people to remain on their mailing lists. Several companies outside of the European Union, however, took the nuclear option to ensure compliance: They blocked all European users from their servers—some temporarily, others permanently.

Tronc Inc., publisher of the *Los Angeles Times*, *New York Daily News*, and other U.S. newspapers, was among those that blocked readers in the European Union from accessing sites, as they scrambled to comply with the sweeping regulation.

"We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market," Tronc said in notices it displayed when users attempted to access its news sites from the European Union on Friday morning.

Some tech firms—which one may have assumed would be the most likely to have the IT capability to comply—halted services as the deadline date hit.

Instapaper, which enables users to save articles to read at a later date, disconnected European customers a day before GDPR came into force.

Other companies have taken a more permanent approach. American media network A+E has blocked EU visitors from all its Websites, including History.com, and some multiplayer online games, including Ragnarok Online, have switched off their EU servers.

Unroll.me, an inbox management firm, announced it was completely withdrawing services for EU companies due to an inability to offer its product—which is monetised by selling insights gleaned from reading users' e-mails—in a way that was compatible with EU law. "We are truly sorry that we are unable to offer our service to you," the company told EU users.

Klout, a social media analytics service, and Super Monday Night Combat, an online game, announced they were also shutting down. Lithium, the owner of Klout, said: "Klout no longer made sense as a standalone service. The upcoming deadline for GDPR implementation simply expedited our plans to sunset Klout."

Other firms have not gone so far as to blame the new regulation but have closed EU operations with convenient timing. Crowdpac, a political fundraising organisation set up by Steve Hilton, once an advisor to former U.K. Prime Minister David Cameron, announced it was closing its U.K. wing "for business reasons" until further notice, adding in a later post that it "hopes one day to be back."

While data experts expected GDPR compliance to be low or problematic in some companies or industry sectors based outside of the EU, they admit that they were caught off guard by the actions of those organisations that just cut off access to EU citizens, or simply pulled the plug on their services.

"I think these actions took almost everybody by complete surprise," says Peter Gooch, partner in cyber-risk services at Big Four firm Deloitte. "It is difficult to see why some companies may have chosen this as a preferred route over trying to comply."

Callum Sinclair, partner and head of technology and commercial at law firm Burness Paull, says that companies should not have been caught off guard by the need for change or have had to resort to "blunt" methods such as geo-blocking.

"Businesses have had two years to get ready since the EU regulation was first agreed, so it really should not have been a surprise to them," says Sinclair.

"What does it really say about the data-handling processes of these companies that have been in place for years if they cannot respond to such a regulatory change in a timely manner?" says Sinclair. "It is hardly a vote of confidence if they are not backing themselves to comply with a best practice regime like the EU's," he adds.

Nigel Tozer, GDPR specialist at data protection and information management software company Commvault, says that tech firms, whose own business model is based on harvesting personal data for their own use, have "shown their true colours" by blocking EU customers because of GDPR.

"If you can't make a 'honest buck' without exploiting people's data beyond what is reasonable, then you don't have a business," says Tozer. "Hopefully, it will alert their customers in the U.S. and other parts of the world to their bad practices," he adds.

Other data experts are equally scathing and skeptical of the approach. Egil Bergenlind, founder and CEO of data management software provider DPOrganizer, says that "essentially, these companies deemed compliance with the new regulation to be too difficult and costly to the extent that they are now willing to lose out on custom."

"While not illegal—and not unsurprising—this is a big problem. For those of us in the EU, it means we lose access to great products and services, which was certainly never the intention of GDPR," says Bergenlind. "But beyond this, by choosing to bow out, these companies very clearly tell their customers in the U.S. and outside of the EU who still use their services that they are not prepared to give them the same privacy rights that people in the EU are now enjoying."

Yet preventing access to services for EU customers does not ensure compliance with the GDPR, or prevent a company from being subject to it, say experts, so the whole exercise could be dangerously flawed. Robert Wassall, data protection lawyer and head of legal services at cyber security specialists ThinkMarble, says that "those businesses blocking their sites will still have to handle any existing EU data in line with the GDPR, unless they delete it or anonymise it."

He also says that in the case of the U.S. news sites, “they may have got this wrong and misunderstood the GDPR.” Wassall says that although the GDPR has a territorial scope beyond the EU, it only kicks in where businesses demonstrate an intention to offer goods or services to people in the EU, as opposed to actually offering goods or services to EU citizens. This is quite a significant distinction, he says.

“For example, is the Chicago Times intending to provide news for EU citizens, or is it simply available to them via the internet? Although intent can be inferred by the language or currency used, the GDPR states that intent cannot be inferred from availability of a Website or e-mail address. In any event, simply offering news does not involve processing personal data of readers,” says Wassall.

He adds, however, if EU residents can (and do) subscribe to these U.S. media outlets, then by collecting, for example, contact details of subscribers, the outlets would be processing personal data, which means they would be subject to GDPR. And on a purely commercial level, Wassall says that these media outlets could potentially face contractual issues with regards to any subscribers they may have based in the European Union, or advertisers who expect to reach an EU audience.

Oana Dolea, GDPR practice lead at legal data consultancy D2 Legal Technology, believes that “the way that some organisations have reacted to the GDPR is not only rash but, most importantly, it is not future-proof.” She adds that some U.S. companies may prefer to explore Privacy Shield certification (a cross-U.S./EU initiative that certifies that U.S. companies can comply with the EU’s data rules) instead of trying to comply with the GDPR, but this takes time, warns Dolea, and any organisation seeking such certification has to meet specific criteria.

Dolea says that the question as to whether curtailing access to services successfully circumvents the applicability of the GDPR depends in great part on what these organisations are doing with the data of their readers/customers behind the scenes. “As part of their strategy of making their services unavailable to EU residents, are they also deleting the data of old EU account holders or other users that they hold? If they are not, they will not be compliant with the GDPR,” she says.

Dolea says that those organisations that might want to pull the plug on their EU customers need to consider some key questions. “Does the technical process by which these organisations are excluding EU residents from accessing their online services involve the processing of those EU residents’ personal data? Are they doing so by using their subscribers’ or previous users’ cookies information or other personal data to know who and where they are, in order to exclude them, or using geo-blocking technology that recognises and blocks IP addresses based in the European Union? In either event, it can be said that that the organisation is using personal data to exclude EU residents from services—but this amounts to processing of EU residents’ data and so the GDPR applies.”

And simply blocking EU readers from access to their Websites does not constitute GDPR compliance, adds Dolea. Advertising may also may have an impact, she says: If online news sites have not adjusted their marketing processes to ensure they do not advertise the newspaper itself to EU residents, or prohibit EU residents from placing advertisements on their news site and even in the paper version of the newspaper, these media companies could be in breach of GDPR rules.

Sinclair believes that it is “almost certainly not compliant with GDPR” to block access to services where any degree of processing of EU citizens data is still happening—for example, where accounts have been suspended but customer details are still being held or archived on service or marketing databases (including by any sub-processors of these companies). “Some companies might even be in breach of their own terms and conditions for withdrawing services at short notice, though they may have given themselves some latitude in their terms,” he says.

“Geo-blocking is a blunt instrument, and its use is highly ironic at a time when the EU is bringing in new rules to prevent it within the EU as it is deemed to be a discriminatory practice,” says Sinclair. “Hopefully this is a short-term phenomenon and we will start to see these businesses making their services available to EU citizens again, and doing so in a way which is more responsible and respectful of individuals’ privacy rights,” he adds.

Experts believe that trying to exclude EU customers from a company’s service offerings is short-sighted. “In the short term it will almost certainly mean an irate customer base not able to access the range of services they ought to be able to,” says Sinclair. “It is also a missed opportunity for these businesses to develop a relationship of trust and intimacy with their customers, while driving business intelligence and customer insight in a responsible way and properly leveraging the value of their data assets."

If other companies follow suit, says Wassall, there will be fewer goods and services available in the EU, but also fewer organisations that are unwilling, or unable, to respect people's privacy and protect their data. "This should be a positive," he says.

Dolea agrees. "The adoption of this exclusionary approach could be damaging to organisations that assume they have resolved their non-compliance problem in this manner, without having done the full analysis," she says.

"The GDPR is meant to incentivise companies to facilitate individuals' ability to control how their data is processed—it should not be pushing companies to make hasty decisions that will be detrimental to their business operations," says Dolea. "One thing is for certain: Putting privacy considerations aside, excluding the entire EU market is not a sustainable long-term solution to a GDPR non-compliance problem, even assuming that this approach is a compliant solution to begin with," she adds.

GDPR flashpoints

- Companies based outside the EU that provide services or goods to the EU (including for free) are subject to the Regulation. These companies may need to appoint a representative in the European Union.
- Consent to retain and process a person's data must be "freely given, specific, informed and unambiguous." Consent must also be demonstrated by a "clear affirmative action by the data subject."
- Maintaining and enforcing internal data protection policies and procedures is a requirement under the GDPR. Companies may need to produce this documentation in the event of a complaint.
- Data breaches and subsequent investigations must also be documented.
- The GDPR imposes new breach notification requirements. Organisations now have 72 hours to report to their nominated national data protection authority, unless the data controller can demonstrate "that the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals."
- Breaches must be disclosed to the affected individuals "without undue delay if the personal data breach is likely to result in a high risk" to their "rights and freedoms."
- The GDPR creates a new "super-regulator" in the form of the European Data Protection Board, which includes the head of each EU member states' Data Protection Authority (DPA). The European Data Protection Board will issue guidance and will be empowered to resolve disputes among the national DPAs.
- Failure to comply with the regulation risks some eye-watering penalties: serious breaches can incur fines of up to €20m (U.S. $24.5 million) or up to 4 percent of global annual revenues—whichever is greater.

—Neil Hodge