Watching

The EU's General Data Protection Regulation creates new challenges for detectives and investigation firms.

When the European Commission passed the General Data Protection Regulation (GDPR) in 2016, it created vast new privacy requirements for personal data, security requirements, and a system that would change the way organizations conduct business in the European Union and across the globe.

In the first year of GDPR enforcement (May 2018 to May 2019), EUROPOL logged that more than 144,000 individual complaints were filed with regulators, more than 89,000 data breach notifications were issued, and more than €56 million in fines were assessed.

"The General Data Protection Regulation is bearing fruit," said Věra Jourová, then EU commissioner for justice, consumers, and gender equity, in a statement on the one-year anniversary of the GDPR enforcement. "It equips Europeans with strong tools to address the challenges of digitalization and puts them in control of their personal data. It gives businesses opportunities to make the most of the digital revolution, while ensuring people's trust in it."

But the regulation also created concerns among the investigations community about whether they would need to notify principals that they were being investigated.

"We routinely conduct investigations without the counterparty's approval," says Don Aviv, CPP, PCI, PSP, president of Interfor International, a corporate intelligence agency based in New York City. "If the counterparty is aware of the investigation and doesn't authorize you to retain their information, what can you do?"

the Watchmen

ILLUSTRATION BY TAYLOR CALLERY

GDPR Basics

The European Commission passed the GDPR in 2016 and created a two-year window for organizations to comply before it began to enforce the regulation in May 2018.

The GDPR requires EU member states, as well as any organization that processes data in the European Union or processes personal data of individuals residing in the European Union, to collect personal data for only specified, explicit, and legitimate purposes. The data must be processed lawfully and fairly, be collected only for relevant—not excessive—purposes, and be accurate.

Personal data must also be stored for no longer than necessary, and organizations must adopt safeguards to secure personal data—including protecting it from unauthorized or unlawful processing, against accidental loss or destruction, and introducing technical and organizational measures to protect access.

In most instances, organizations and institutions subject to the GDPR must obtain consent for collecting and storing someone's personal data. They also, generally, must erase an individual's data if he or she requests the organization to; additionally, institutions need to make an individual's data available upon request, except in certain circumstances.

Organizations are also required to conduct risk assessments for data they store, follow data breach notification mandates, and extensively log why they are collecting an individual's data.

However, there are exceptions. For instance, the GDPR specifically outlines that law enforcement and national security agencies are not required to obtain consent from individuals to collect their data.

"Any processing of personal data must be lawful, fair, and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law," according to the European Commission. "This

does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security…"

Authorities must create and maintain safeguards to protect the personal data they collect from being wrongfully accessed or distributed. Unlike other organizations, law enforcement may keep and not delete data.

"…it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection, or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected," according to the European Commission.

And, unlike most organizations, law enforcement agencies can decline to share the data they collect on an individual with that person—as long as those refusals are shared in writing and explain the factual or legal reasons why the data cannot be shared.

"Member States should be able to adopt legislative measures delaying, restricting, or omitting the information to data subjects…to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection, or prosecution of criminal offences, or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others," the European Commission explained. "The [data] controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted."

Contract Investigators

While the European Commission has laid out how law enforcement is impacted by the GDPR, it has not done so as explicitly for private investigators. Various groups raised concerns about how the regulation would impact the private sector's ability to carry out investigations when the GDPR was adopted in 2016, says Jane Shvets, partner in the White Collar and Regulatory Defense Group at Debevoise & Plimpton.

Shvets, who works with clients in both London and New York, advises clients on data protection and cybersecurity matters, along with a focus on white collar defense and internal investigations. After the GDPR compliance deadline, Shvets says that everyone is paying more attention to data protection due to the large fines that regulators can assess on violators—up to 4 percent of annual global turnover.

The company has to represent to that investigator that all the data is compliant with GDPR.

The requirements the GDPR introduces for investigators present challenges, but "I wouldn't say they present an insurmountable hurdle," Shvets says. "There may be a lot more hoops that you have to jump through to get there."

One core component of the GDPR is the transparency principle—that individuals have a right to know if their personal data is being collected, how it's being collected, and for what use. But there is also a provision in the GDPR that says the transparency principle applies—in some cases—if it does not defeat the purpose that the data was being processed for, she explains.

"You could argue that if someone was committing fraud or engaging in misconduct, you have a strong basis of why you should not alert that individual to the steps you are taking to investigate them," Shvets says.

Also, if a company is investigating an employee, it may already have a legal right to collect information on that individual which can be stored and processed.

"Usually, employment contracts have something in them to the extent that the employee is using firm email or Internet, and the company has a right to monitor that—there is no reasonable right of privacy," Shvets says. "In the EU, many organizations have that in their employment agreement."

When it comes to hiring an outside investigator, an organization's legal team should be involved to help guide the process and ensure that the contract outlines requirements that are compliant with the GDPR.

"We're a law firm and we often work with investigative outlets when a client decides to do an investigation," Shvets says. "We're the ones who engage these firms on clients' behalf, and we're seeing significant attention to data protection…the company has to represent to that investigator that all the data is compliant with GDPR."

This means that the investigations firm is appropriately protecting data collected for the client to prevent unauthorized access, such as encrypting the data and keeping it password protected. Firms must detail if the collected data is transferred to any third parties during the course of their work for the client.

"In my experience, they usually have extensive provisions about the measures they take to protect client data," Shvets adds. "And companies are increasingly requesting such measures. It's not just you get the data and you're home free. You have to protect the data and then dispose of it. You're not allowed to keep it longer than necessary."

Organizations can also deny sharing data with individuals who have been the subject of an investigation. However, this is more difficult for investigations firms that are working on behalf of a company; they will need to have a

ASIS INTERNATIONAL
Advancing Security Worldwide®

Your Best Source for ASIS Certification Study Resources

Is attaining one or more globally recognized board certifications a professional goal? Choose from ASIS International's best-in-class resources and study materials to help you prepare for the exams.

- Recommended reference materials
- Variety of delivery formats
- Updated to reflect most current exam domains
- Developed and approved by ASIS

Whether you prepare on your own or join a group of peers to study together, you can mix and match from a variety of offerings to fit your learning style and schedule.

Learn more at **asisonline.org**

"This morning I sat for the PSP exam and passed, in no small part due to the excellent, thorough, and engaging instruction during the PSP review course."

—Jane P. B. Hozier, PCI, PSP, Assistant Director, Operations and Analysis, The Human Intelligence Group

reason for denying the request to share the data with the individual.

One reason would be legal privilege. Another would be if the organization found evidence that the individual committed a crime and turned the data over to law enforcement.

"Or if the documents also contain personal information of other individuals," Shvets says.

The Impact

While the GDPR poses new challenges and paperwork requirements for investigators, it does not limit the scope of their work, says Roger Bescoby, director of compliance and development at Conflict International Limited in London.

When the GDPR was approved in 2016, his firm produced documentation and advisories to educate staff—and clients—about how the new regulation would affect their work.

The biggest change, Bescoby says, is the need to have a clear audit trail to show how the firm is conducting its work in a manner that is compliant with the regulation. The firm begins this process when a pitch is sent by a client outlining the scope of what it is looking for. The firm will then create a cost estimate, conduct an impact assessment, and explain if the case is justifiable—or not.

"The best way I had a regulator describe it to me was it's like when you were a kid and you had an exercise book—you had to show your work," he explains.

A key part of this, which Shvets also emphasizes, is to have both the client and the firm outline why this investigation needs to be carried out and the legal reasoning for doing so without informing an individual that they are being investigated.

"If somebody just rings up out of the blue and asks us to find David Jones for me, or a woman he met on holiday, that person could have the wrong reasons to want to find that person," Bescoby adds. "We have to establish if there's a

SECURITY GUIDANCE AND THE GDPR

The EU's General Data Protection Regulation (GDPR) is lengthy. It contains 99 articles that lay out data rights for individuals, requirements for organizations that collect and process personal data, penalties for noncompliance with those requirements, and more.

In addition to the regulation itself, the European Commission has released guidance for certain industries on best practices for implementing the GDPR. The commission, however, has not released specific guidance for the investigations industry and private security; it could release additional guidance in the future.

But some EU member states regulation enforcers have issued guidance for the security industry on implementing the GDPR and other data privacy requirements.

One example is the United Kingdom, which as of *Security Management's* press time had not left the European Union. To implement the GDPR, the United Kingdom enacted the Data Protection Act (DPA).

The UK's Information Commissioner's Office (ICO) is charged with oversight of these privacy regulations and has created a page on information rights obligations for those working in the criminal justice sector. These resources offer guidance on how to implement the GDPR and the DPA when using surveillance technology—including when wearing body worn cameras or using unmanned aerial systems.

Roger Bescoby, director of compliance and development at Conflict International Limited in London, has regularly reached out to the ICO for clarification on compliance and implementation of the GDPR.

He recommends that security professionals with questions about the regulation, particularly its scope, reach out to their regulatory body to gain insight.

"It's a very, very difficult piece of regulation to understand and work with," Bescoby adds. "Speaking to the ICO, they understand the complexity...and they are all about helping people before prosecuting them."

ILLUSTRATION BY ISTOCK

legitimate reason for this process to take place. Is it necessary for the performance of the contract?"

The GDPR has also helped "clean up" the industry a bit, Bescoby explains, because businesses must demonstrate their attitude towards compliance and enhance the security around the data they store. They are now required to log the data they accessed and who that data was shared with.

While this process creates an audit trail for regulators to understand why and how firms are storing data, it also creates more work for investigators and their staff—which can increase costs, Aviv explains. "We are drowning in paperwork," he adds.

It's like when you were a kid and you had an exercise book—you had to show your work.

Bescoby and his CEO are both members of the World Association of Detectives. Because of this connection, Bescoby has given numerous presentations to investigators about the GDPR and how it impacts their work.

One thing that continues to surprise him is that many individuals think their organizations are not subject to the regulation because they are not investigating an individual in the European Union.

"The biggest misunderstanding of GDPR that I found when I was doing talks was that because it came out of Europe, it only applied to the EU and its citizens," Bescoby says. "That is wrong. It applies to anybody."

And to confirm, Bescoby wrote to the Information Commissioner's Office (ICO), the independent body that upholds information rights in the United Kingdom. The ICO explained to him that the GDPR applies to any organizations and institutions that control and process EU data.

"You can have a Chinese man living in Norway—it doesn't matter where he's from or where he lives, if that data is processed within the EU, it's subject," Bescoby says.

MEGAN GATES IS SENIOR EDITOR AT *SECURITY MANAGEMENT*. CONTACT HER AT *MEGAN.GATES@ASISONLINE.ORG*. FOLLOW HER ON TWITTER *@MGNGATES*.