WHITE PAPER

# DECEPTION AND THE GDPR

TRAPX SECURITY

# Deception and the General Data Protection Regulation

## Contents

## Executive Summary

- The General Data Protection Regulation offers a valuable opportunity to re-appraise approaches to security, and challenge existing methods of operation
- Participation in the GDPR requires a shift from 'compliance-driven' checkbox activities to entering the spirit of the privacy dialogue
- Privacy by Design, breach reporting, and Cloud-based business models are significant factors to account for in planning for GDPR
- A new pragmatism is required among organizations that acknowledge the increased risk of GDPR-related data loss from advanced attackers
- Novel security approaches like Deception Based Cybersecurity are invaluable weapons to organizations seeking to secure personal data and avoid heavy fines

## The General Data Protection Regulation – A New Level of Stringency

The General Data Protection Regulation comes into force on 25th May 2018 and represents significant changes to the legal framework governing data privacy in the European Union, including giving authorities the ability to take tough action on companies that flout the rules. Originally proposed by MEP Viviane Reding in 2012, the new laws include provision for the privacy and use of EU citizens' data, with a separate directive governing the use of an individual's data by law enforcement agencies.

Replacing the Data Protection Directive (Directive 95/46/EC) of 1995, the GDPR has lineage in Article 8 of the European Convention on Human Rights dating back to the fifties, with a guiding principle of respect for one's 'private and family life, [their] home and [their] correspondence'. The objectives of Directive 95/46/EC were to further 'protect the fundamental right to data protection and to guarantee the free flow of personal data between member states'. After strong lobbying from privacy advocates, the EU recognized that huge technological shifts have transformed the landscape. Paradoxically, while many citizens seem very happy to share vast amounts of personal data via social media, trust in the ability of companies to protect this information came to be viewed as potentially harmful to economic growth. Personal data protection was explicitly named as having a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 strategy.

Data protection is not just an EU mandate either and is far from being globally agreed. The framework embodied in the U.S. Safe Harbor Privacy Principles and its strong focus on self-certification was called into severe question when it was declared invalid by the European Court of Justice in October 2015. This resulted in a rethink of privacy laws governing the exchange of personal data between the US and EU, resulting in the EU-US Privacy Shield which was not initially unconditionally ratified until July 2016. The future of the EU-US Privacy Shield is largely considered uncertain because it features strikingly different regulation mechanisms and a focus on market forces rather than citizens. It seems likely that the more stringent GDPR mandates due next year will force a reappraisal of the Privacy Shield moving forward.

## Brexit and GDPR

The decision of the UK government to leave the EU has led to a great deal of confusion about whether GDPR compliance is necessary for UK businesses. However, with Article 50 triggered in March 2017, and the exit process likely to take up to two years, it seems clear that there is at least a one year window during which UK organizations will have to comply with the mandates. Additionally, data privacy is likely to form a cornerstone of the deal that the UK must negotiate with the EU in order to retain access to the single market. Suffice to say, the EU themselves are already very vocal about the need for organizations to comply if they are looking to 'process data about individuals in the context of selling goods or services to citizens in other EU countries'.

## What does it mean to your business?

One of the most well-publicized parts of the new GDPR are the potentially business-crippling fines that could result for organizations who lose customer data, particularly if they demonstrate a lack of commitment to the controls and guidelines intended to minimize that risk. The Payment Card Industry Security Standards Council estimated that in the UK alone, organizations in 2015 would have been fined £122 billion. With data breaches continuing to rise, the prognosis for organizations that do not properly enshrine the guidelines alongside effective security controls is very poor indeed. However, it is clear that the highest fines likely to be levied under the new regulations (4% of global turnover or €20million), will be reserved for organizations that fail to consider even basic compliance as critical to fulfilling the spirit of GDPR. In other words, it is the organizations that get things *very* wrong that will be likely to incur these sorts of penalties. However, any compliance breach around GDPR could still be very costly, both financially and reputationally. Additionally, with penalties of this scale, it could be argued that organizations historically targeted by nation states or by criminal syndicates could see a rise in so-called 'hacktivism'. The potentially seismic effect of GDPR-scale fines on business operations is a far more tangible way of getting an organization's attention than traditional methods such as crashing websites or leaking intellectual property. It is perfectly plausible that an organization could be put out of business if it were to fall sufficiently foul of the GDPR legislation following a material breach.

Finally, some of the imperatives placed on modern corporates by GDPR will substantially increase costs associated with breaches, and not just because of the scales of the fines. As will be explored later in this document, the new rules on notifications following a data breach will significantly impact the incident response process, substantially increasing the administrative overhead as teams seek to identify the scale of the breach and who needs to be notified.

## Privacy by Design

That said, there are several underpinning principles that the GDPR is founded upon, and which should be considered such minimum requirements to both minimize the chance of data loss and also mitigate the scale of fines incurred in the event of breaches. One of these is 'Privacy by Design'. Explicitly named in the guidelines, Privacy by Design (PbD) was created by Ann Cavoukian, then Information and Privacy Commissioner of Ontario, Canada in 1997. PbD asserts that privacy cannot be delivered by compliance alone, but that it must be delivered as part of an organization's default modus operandi. Indeed, many of the commentators discussing PbD suggest that only a true appraisal of the impact on the *individual* of a data breach, rather than a business assessment truly falls within the spirit of Privacy by Design.

Cavoukian herself forwards seven fundamental principles that should be considered fundamental to privacy assurance;

1. Proactive not reactive; Preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

It is within these principles that the clearest guidance for technology teams about the supplementary controls that would optimise an organization's GDPR position are found. The first item discusses anticipating and preventing privacy invasive events before they happen. This is a critical point; PbD does not offer remedies for those events which have already happened, it undertakes to prevent them happening in the first place.

Additionally, Privacy by Design then introduces the concept of Privacy by Default. This is also explicitly referenced in the GDPR and stipulates that only data required for the task at hand and that the person to whom the data relates needs do nothing to preserve its integrity. This means protective controls to ensure that such data remains private, and the opportunities for attackers to access the data are minimized. This segues into the next guideline which describes the need for *embedded* privacy. In other words, the ground-up design of systems and processes that minimise the chance of data being compromised and privacy breached, including testing against hackable vulnerabilities in supporting software like injection attacks. Privacy becomes a core deliverable of compliant systems and their surrounding controls, meaning that no trade-offs between security and privacy should need to be made introducing the idea of 'positive sum'. Cavoukian describes that all objectives for privacy should be achievable, and none should be mutually exclusive.

Lifecycle security is a significant component of PbD and stipulates the end-to-end management of private data, including its secure destruction at the end of its life or when demanded by the individual, according to the provisions laid out in the 'right to be forgotten' clauses. Also explicitly covered in the Lifecycle component is the notion of strong security measures embedded into the process from the start to finish.

Finally, PbD moves on to discuss transparency, openness and a regard for user-centricity in execution. The true spirit of Privacy by Design is that dogged adherence to compliance mandates rather than pursuing policies and investment decisions that support the individual are likely to fail. Worse than that, failing to embrace the spirit associated with PbD as set out as part of GDPR is likely to ensure that auditors and investigators take a dim view and react with the full power of the legislation in the event of a breach.

## Breach Notification

The GDPR will impose strict rules on the process of notification if a data breach occurs, specifically, if a data breach is considered to have a detrimental effect on the rights and freedoms of individuals then the regulatory authorities must be notified within 72 hours of the organization becoming aware of the breach. Additionally, significant effort is required in ascertaining whether the data lost constitutes a notifiable breach. For example, if an organization loses data that could result in identity theft, then the supervisory authorities must be notified. However, if a staff telephone list was lost, this would not require notification. This means a considerable additional administrative overhead associated with the Incident Response effort. Once a data breach has occurred, not only will the standard forensics and attribution activities have to be conducted, but an extensive audit of the data lost, and if necessary notification of the regulators and the *individuals* concerned.

The most significant challenge associated with this particular clause is the fact that awareness of a breach for most modern organizations is almost as likely to come from an external as an internal source. Mandiant's 2017 M-Trends report suggests that 47% of notifications of a breach will be external, following median attacker dwell times of 99 days. The legislation states that the onus to notify the supervisory authorities begins at *awareness* of the breach, but with dwell times over 30% higher for organizations notified by external sources, it seems likely that these are the companies that will be most firmly treated by the regulators. It is also clear that a substantial revision of Incident Response procedures to address the assessment of a data loss and the associated processes for regulatory and individual notification will be critical.

## Shadow IT and the Cloud Providers

Even with Privacy by Design in place and a commitment (both in spirit and procedurally) to swift and effective notifications in the event of a breach, there remain additional complexities around GDPR, specifically in relation to Cloud providers and their compliance position. With organizations of all sizes now wholly embracing the benefits of outsourced compute platforms, or even those with hybrid operations, the landscape becomes increasingly complex. The GDPR makes extensive changes to existing privacy laws that draw a line between the responsibilities of Data Controllers and Data Processors. Under the new legislation, the Data Processor or third-party agency expressly permitted by the Data Controller has the same responsibilities for data protection as the Controllers. This will radically increase the risk profile for cloud and data center providers acting as data processors. It also means that the provision of shadow or non-centrally authorized cloud services could create the sorts of data protection loopholes in organizations that could result in extremely costly fines and reputational damage. Under the accountability principle set out in Article 5(2) of the GDPR, an ongoing demonstration of compliance, arguably which includes constant revision and update of the underlying security controls is mandated. These governance challenges, along with a clearly stated need to constantly demonstrate compliance in an ever-changing technical landscape dictate a creative and ongoing commitment to new methods of securing Personally Identifiable Information from attackers.

## The New Pragmatism

With the potential costs of breaches placed so front of stage within the GDPR framework, the surrounding security landscape must be re-evaluated. To repeat a metric stated earlier, the Payment Card Industry Security Standards Council estimated that British firms in 2015 would have incurred $112bn in fines because of poor compliance with GDPR standards. However, GPDR itself does not offer substantive guidance on how to minimize the chances of a breach, or of critical data actually being exfiltrated from the network. Rather, it gives a set of policies and a spirit with which to approach the issue of compliance. The central question in this paper is whether the sum effect of existing security frameworks like Defense in Depth, plus the threat of potentially fatal compliance fines and the guidelines offered by the GDPR will actually translate to a more sophisticated security posture that actively keeps attackers out of the network?

Data breaches continue unabated. In 2016, 167 million LinkedIn records were posted on the dark web (following the 6.5 million encrypted passwords that were lost in 2012), Verizon lost information relating to 1.5 million enterprise clients, Tesco Bank had the accounts of 20,000 of its customers raided and most recently in 2017, Wonga.com the payday loan company, reportedly lost over 200,000 bank accounts and sort codes. With backdoors available for purchase from hackers and criminal syndicates into many of the major corporations, and with the richest possible supply of online information for spear phishing purposes available from Facebook, LinkedIn and Instagram, the chance of an attacker gaining access to a corporate network is a likelihood, rather than a possibility.

This is a critical point. Having an attacker active on a company network does not immediately translate to a crippling GDPR fine, nor does it necessarily spell disaster for a company's value as when TalkTalk lost 7% of its value following a successful hack. When an attacker achieves a point of persistence on an infrastructure, he will need to perform reconnaissance and ultimately move laterally to higher value targets before actually being able to exfiltrate data. It is at that point that the situation has become terminal.

Sophisticated attackers are increasingly cognizant of the risks presented to them after they have successfully breached a network. Achieving that first foothold can be an expensive process, either by procuring access to a network or by developing custom payloads and sophisticated spear phishes that capitalize on human factors to ensure success. A long history of Intrusion Detection Systems has made attackers extremely efficient at performing reconnaissance on networks, either relying on extremely stealthy scanning of a network on well-known ports or by performing host-based reconnaissance on the compromised client to identify the next targets. Lateral movement is even harder to detect through the use of well-known corporate standard tools like PowerShell, psexec and WMI, but it should be borne in mind that attackers WILL need to move laterally to gain access to GDPR-sensitive information, and that is when they are most vulnerable to detection. Given that attackers will be anticipating targets to be investing heavily in data protection, they will likely be researching countermeasures and seeking to reinforce their ability to gain privilege escalation. The 2015 Mandiant M-Report suggests that attackers can achieve privilege escalation in as little as three days. This will significantly improve their ability to circumvent the protection offered to Personally Identifiable Information in pursuit of GDPR compliance.

## Time to Detect – A New Service Level for Security

As has been mentioned earlier, dwell times have been steadily decreasing year on year, but are still too high, with the first point of awareness often being an alert that data is being

moved off the network. Clearly, for organizations that want to avoid the most punitive repercussions from the regulators, the service level for awareness of an attacker on the network must inexorably trend to as low a level as possible. Only this way can an attacker moving through the network with elevated privileges be prevented from accessing, exfiltrating and disseminating GDPR-sensitive data.

In support of this end, novel approaches to security must be leveraged. With the knowledge that attackers are ever-more motivated by Personally Identifiable Information, and that organizations are more susceptible to the consequences of its loss, how can the security professional maximise his chance of detecting an attacker and minimize the compliance exposure to his employer?

## Deception Based Cyber Security – At Enterprise Scale

One method is to use Deception based approaches. Deception is now seen as a fresh approach to complement existing security investments. Organizations have begun moving from the 9:1 ratio of prevention-to-detection toward the 6:4 ratio advocated by many security thought leaders. A Deception infrastructure is the best way to identify attackers' positions and gain valuable information about their techniques, tactics, and procedures.

So, what is a Deception Infrastructure? The idea of Deception in all forms of warfare is not a new one. In explicitly military contexts, fake sonar signals and fake radar for the navy and air force respectively are well-established to convey false information to adversaries. Similarly, fake reconnaissance information about ground troops' movements is also commonly employed. It should also be argued that cyber attackers routinely use Deception to further their causes. What is a spear phishing email, if not a Deception? The use of Deception-based technologies in modern organizations is increasingly seen as a legitimate tactic against advanced cyber adversaries, where existing Defense-in-Depth approaches have largely failed to make the grade. Different classes of Deception technology have been in use for many years, and include placement of vulnerable assets at key locations on the infrastructure so that attackers looking for targets to move laterally to can interact with such systems and trigger alerts. However, the use of dedicated workstations or servers for this purpose incurs hardware and operating system costs. For such approaches to succeed at scale, in large organizations with GDPR-qualifying assets under their custody, the price incurred by these highly manual approaches is high. Once the attendant costs of integrating with the wider security ecosystem and the work associated with deriving meaningful telemetry are considered, the approach becomes impossible to cost-justify and maintain.

Conversely, the placement of relatively unsophisticated 'low-interaction' devices can deliver value from being able to respond in a rudimentary fashion to network scans and connection attempts. Such mechanisms are relatively easier to scale, but offer little telemetry on the advanced attacker and are easy to fingerprint and avoid.

Additionally, given that attackers are increasingly performing local reconnaissance on compromised machines, rather than risking detection by Intrusion Prevention Systems, any attack that does not begin on the network might be missed.

With these limitations understood, a new generation of highly integrated and interactive Deception solutions have come to market, which leverage deployment at scale, convincing attack surfaces for hackers, and consolidated telemetry integrated into the wider ecosystem to deliver maximum value to alert-fatigued security operatives.

At the most basic level, lures or tokens are used to blanket the infrastructure, client and server-side. Deployed at scale, these tokens and lures are meant to permeate the network with fake assets that encourage attackers at the reconnaissance stage to move laterally. Tokens are essentially a response to the notion that advanced attackers no longer perform noisy network scans. If they do network scans at all, they avoid detection by using single-packet connect requests on well-known ports at an extremely slow rate.

Attackers are now far more likely to concentrate on information they gather from the endpoint; once they're on an endpoint, they can escalate privileges and move to other systems silently. Tokens are an incredibly valuable part of the story, but they're only the beginning. Imagine if an attacker doesn't follow the lures or understands that certain Deception solutions use scheduled tasks to set up the lures. Scheduled tasks are one of the first ways an attacker will try to establish persistence, in which case the Deception trail runs dry very quickly.

An additional layer is critical to deceiving at scale, offering a far broader attack surface and a much higher probability of engaging an attacker. This layer blankets the environment not with tokens, but with emulations of actual systems. Indistinguishable from the real thing, an emulation-based component to the solution offers attackers an interactive experience, fake data, and the ability to pass through seamlessly to a very realistic, high-interaction system that can record all attacker activity in real time. An emulation layer offers commodity IT assets and devices that represent newer vectors, including Internet-of-Things devices, medical devices, SCADA systems, and automated teller machines (ATMs). Realistic, inter-trap traffic increases the realism to network-focused attackers.

Finally, and most critically to GDPR compliance is the notion of fake data. With attackers mobilising to gather personally identifiable information (PII) from all available targets, a good Deception Infrastructure allows users to lay down a convincing blanket of worthless, but highly compelling information to attackers. These can be fake databases, fake documents describing customer account details, network schematics, intellectual property, credit card details. Deceptive documents can be configured to beacon back to the Deception Infrastructure if they're taken off-premise. This dense, rich and interactive fake IT framework which can alert on the slightest interaction becomes an extremely effective way of identifying attackers or insider threats on the network and looking for the sort of information that could damage reputation and profitability if it were to get out.

By placing a combination of tokens, emulations, full operating system decoys and fake data onto the environment, attackers will be unable to discern the real from the false and reveal their position and their tactics. Additionally, integration into the wider security ecosystem, and into automated forensics tools to gather critical information about the machine used by the attacker to compromise the environment is available.

Finally, it is important to note that alerts from Deception technology are generally of the highest accuracy and integrity. No one should be interacting with the decoys and fake data.

These alerts are almost always good indicators of an ongoing cyberattack or insider threat activity inside the network. In contrast consider the virtual flood of alerts from other defense in depth security components inundating most security operation center (SOC) teams today.

So, how does Deception support organizations looking to participate in the spirit and the compliance requirements for GDPR? How can it serve to mitigate the crippling fines potentially to be levied against those companies that do not take such mandates seriously? Simply put, Deception is an acknowledgement that attackers fully understand the potential rewards of a successful cyber-campaign against a target organization. As a result, they are more determined, persistent and resourceful than they have ever been, now using well-trusted tools like PowerShell and psexec to further their causes. This means that organizations expecting to be breached are now turning their attention towards solutions that offer novel ways of detecting breaches early, and deriving maximum telemetry on threat actors. Deception speaks explicitly to the stipulations made in Privacy by Design that proactive operations are best. It addresses the need for embedded privacy by allowing organizations to factor in Deception operations at the very earliest phases of new projects and ventures. Deception also means that teams seeking the earliest possible alerts to breach detection can mobilize quickly to minimize the chance of attackers who have breached the perimeter gaining access to sensitive GDPR-qualifying data. Finally, Deception allows organizations who use outsourced services to provide additional layers of protection in their cloud infrastructures to ensure that business partners do not inadvertently offer attack vectors to attackers looking for critical data in third-party repositories.

## In conclusion

GDPR represents a substantial change in the way that regulatory authorities will police and enforce safety around customer data. Both in support of individual's rights to privacy, but also in support of confidence in the Digital Agenda for Europe and consumer confidence in online trading, it represents significant challenges for even the most progressive organization. However, new approaches like Deception-based Cybersecurity offer such organizations the ability to transform their time to awareness of internal and external threats and protect the very data covered by the GDPR. By adopting additional controls like this, corporate networks can be more effectively monitored for attackers and effectively responded to, augmenting existing security investments, and mitigating compliance risks.


**About TrapX Security**

TrapX is a leader in deception based cyber security defense. Our solutions rapidly detect, analyse, and defend against zero day and advanced attacks in real time. DeceptionGrid™ provides automated, highly accurate insight into malware and malicious activity unseen by other types of cyber defense. We create a proactive security posture, fundamentally changing the economics of cyber defense by shifting the cost to the attacker. The TrapX Security customer base includes Forbes Global 2000 and government customers around the world in sectors that include defense, healthcare, finance, energy, consumer products, and other key industries. Learn more at www.trapx.com.