MORRISON | FOERSTER

250 WEST 55TH STREET
NEW YORK, NY 10019-9601

TELEPHONE: 212.468.8000
FACSIMILE: 212.468.7900

WWW.MOFO.COM

MORRISON FOERSTER LLP

BEIJING, BERLIN, BRUSSELS,
DENVER, HONG KONG, LONDON,
LOS ANGELES, NEW YORK,
NORTHERN VIRGINIA, PALO ALTO,
SAN DIEGO, SAN FRANCISCO, SHANGHAI,
SINGAPORE, TOKYO, WASHINGTON, D.C.

November 28, 2017

Writer's Direct Contact
+1 (212) 506.7213
MWugmeister@mofo.com

Submission to the Article 29 Data Protection Working Party on Guidelines on Personal Data Breach Notification under Regulation 2016/679

We write on behalf of the Global Privacy Alliance (GPA). We welcome the opportunity to comment on the Guidelines on Personal Data Breach Notification under Regulation 2016/679 ("Guidelines") issued by the Article 29 Working Party ("Working Party").

The GPA is comprised of a cross section of global businesses from the automobile, aerospace, communications, computer and computer software, consumer products, electronic commerce, financial services, logistics, and travel/tourism sectors. The GPA works to encourage responsible global privacy practices that enhance consumer trust as well as preserve the free flow of information. Members of the GPA take their privacy obligations very seriously. The views expressed herein generally represent the views of the members of the GPA. While all members support the overall approach presented in this paper, some of the individual points raised may not be relevant to all members.

The General Data Protection Regulation (GDPR) requires data controllers to notify a competent data protection authority (DPA) about personal data breaches and also, in certain cases, the individuals who have been affected by the breach. The Guidelines explain these mandatory breach notification requirements and provide some helpful examples of the types of breaches that may trigger notification under the GDPR. However, we have concerns about two issues addressed in the Guidelines because they exceed GDPR requirements and will make business compliance more difficult: "availability breaches" and the notification timing requirements for the controller when its third party processor has sustained a personal data breach. As explained below, the Working Party's interpretations of these issues greatly expand the scope of notification required and impose unrealistic and overly burdensome timeframes for notification.

I. Availability Breaches

Issues. The Guidelines greatly expand the definition of a personal data breach beyond what is set forth in Article 4.12 of the GDPR. In particular, the Guidelines state that a loss of access to personal data, even a temporary loss of access, which it calls an "availability

breach," constitutes a personal data breach that may require notification to DPAs and affected individuals.

Comments. Under the GDPR, a "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." The reference to "access" pertains to access by unauthorized third parties, rather than the ability of the company to access its own personal data. Furthermore, the concepts of "destruction," "loss," and "alteration" refer to permanent, not temporary conditions.[1]

In contrast, the Guidelines expand the scope of a personal data breach to include any loss of access (by organizations and individuals) to personal data, which is defined as an "availability breach."[2] Furthermore, the Guidelines, citing the GDPR security provisions in Article 32,[3] take the position that while a permanent loss of, or destruction of, personal data will always be regarded as an availability breach, even temporary loss of access requires notification to DPAs and affected individuals if the lack of availability of the personal data is likely to result in a risk to the rights and freedoms of individuals. The Guidelines cite as an example medical records in a hospital that become unavailable for 30 hours because of a cyber attack. In this case, the Working Party believes that both the hospital and the affected individuals should be notified.

Security Incident vs. Data Breach. The Guidelines correctly note that any incident resulting in personal data being made unavailable for a period of time is a security breach (Page 7) but not all security incidents are necessarily personal data breaches (Page 6). The scope of the security and data breach notification provisions are clearly different. A temporary loss of availability without any other event is considered only a service level issue which can be addressed contractually; it should not be considered to be a loss of personal data which may require documentation and potentially notification. Therefore, only situations where

[1] For example, the Working Party Opinion 03/2014 discusses the concepts of "loss" and "alteration" in the context of situations in which the data controller does not have adequate backups. It provides an example of computers containing updated medical records that were stolen. The organization only has old backups of the medical records available; therefore, all of the updated information contained on the stolen computers is considered to be permanently lost.

[2] The Guidelines define an "availability breach" as "an accidental or unauthorized loss of access to, or destruction of, personal data." This definition also exceeds the definition of an "availability breach" set forth in the Working Party Opinion 03/2014, defined as "the accidental or unlawful destruction or loss of personal data."

[3] Article 32 of the GDPR states that when implementing technical and organizational measures to ensure a level of security appropriate to the risk, organizations should give consideration to their "ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" and the "ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."

personal data are lost or permanently unrecoverable should be considered to be personal data breaches.

Temporary vs. Permanent Loss of Access to Personal Data. Under Article 32 of the GDPR, organizations must ensure that they have ongoing access to their processing systems and services and, in the event of a security incident, are able to restore availability and access to personal data in a timely manner. However, the GDPR does not require that personal information subject to processing be made available to the individual at all times. Not only is constant and immediate availability to individuals not required by the GDPR, it is not realistic in most contexts. The GDPR reflects this reality. For example, access rights under the GDPR can be responded to within 30 days (not immediately). Constant access to processed personal data is not an established individual right.

By expanding the GDPR's personal data breach definition to include any lack of availability, the Working Party may be trying to address the growing problem of ransomware; however, unavailability of data may also be caused by technical issues, or may be the result of Internet issues or network problems and many other events that do not compromise the security of personal data. For example, in the case of the stolen encrypted laptop of a financial advisor referenced in the Guidelines, no backup was available but the encryption key was not compromised. Therefore, in this case, there is no risk that the information can be misused. However, the Guidelines provide this case as an example of when notification is required. This example suggests that even if there is no risk to individuals, organizations would have to treat even temporary unavailability as a potential notifiable data security incident. As you know, responding to security incidents is time intensive and requires input from multiple people across an organization. If the incident response team is required to evaluate even temporary unavailability to determine if there is a risk to individuals, that will result in the incident response teams focusing on issues which create no risk to individuals rather than on incidents and situations that are complex and could result in significant risk.

In sum, unavailability of personal data is not the same as a loss of personal data, and, therefore, consistent with the GDPR, should not fall under the definition of a personal data breach and, at a minimum, temporary unavailability should not constitute a breach.

II. Timing of Breach Notification

Issue. The Guidelines essentially eliminate the period afforded to the processor under the GDPR to notify the controller without "undue delay" and replaces it with notice period that must be "immediate." This interpretation creates a number of problems. In particular, it sets up a standard with which it will be impossible for processors and controllers to comply, imposes liability on controllers even if they do everything properly and for events which are out of their control, and is likely to result in excessive (and incomplete) DPA notifications.

Comments. The GDPR requires controllers to provide notice of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become "aware" of the breach. The Guidelines seek to clarify the question of when the controller becomes aware of the breach. The Working Party believes that a controller should be regarded as having become aware when that controller has a reasonable degree of certainty that a security incident has occurred that has led up to the personal data being compromised.

The Guidelines further consider the situation in which the processing is being carried out by a third party processor and the processing is subject to a breach. Under Article 33(2) of the GDPR, the processor must notify the controller without undue delay when it becomes aware of the breach. The Guidelines take the position that in such cases the controller is assumed to become aware once the processor has become aware, regardless of whether or not the processor has informed the controller of this fact. Because the GDPR does not provide an explicit time period within which the processor must alert the controller, the Working Party recommends an immediate notification by the processor with further information about the breach provided in phases as information becomes available.

Unreasonable Notification Standard. Corporate networks are barraged on a daily basis with a variety of security threats such as phishing emails, malware, bots, ransomware, and web attacks. According to an April 2017 report by Symantec,[4] 357 million new malware variants, 98.6 million bots, and 463,841 ransomware attacks were detected and an average of 229,000 web attacks were blocked per day in 2016. In addition, there were 1,209 breaches in 2016, affecting 1.1 billion individuals. The average identities exposed per breach were 927,000. The report also highlights the fact that cyber attackers are becoming increasingly sophisticated, using very simple tools and tactics that can result in symptomless infections and allow attackers to hide in plain sight for months on end.

Given the magnitude of the cyber threats that companies face on a daily basis, an extensive amount of forensics work is often required to detect, confirm, and investigate possible breaches. These investigations take time. The GDPR's aggressive 72-hour notification standard for controllers already poses significant challenges and difficulties for organizations. This standard coupled with the Working Party's replacement of the GDPR's "undue delay" requirement for processors within a required "immediate" period sets up an impossible situation for processors and controllers, one which is likely to lead to noncompliance.

The requirement to provide immediate notice poses very practical and logistical problems. Consider a processor that has thousands of clients. The processor would first need to ascertain that is has been the victim of a breach that impacts personal information. It must

[4] See Symantec's Internet Security Threat Report, Volume 22, issued April 2017, available at https://www.symantec.com/security-center/threat-report.

then must discern which data may have been impacted (this is often not self-evident), and then which of its customers were affected by the breach. Then it would need to identify the appropriate individuals to contact within its customers' organizations and then contact those customers in such a way that the information is received by individuals who are in a position to respond to the information. Particularly when dealing with large numbers of customers and large amounts of personal data, an "immediate" notice obligation is not feasible. The GDPR specifically provides that processors should provide notice without undue delay. The GDPR does not say that the processors must notify the controller immediately, thus imputing the knowledge of the processor to the controller undercuts the plain meaning of the GDPR.

In addition, if the processor attempts to provide notice "immediately" to hundreds of thousands of customers, the information provided would be devoid of useful content. The processor would not be able to provide information about how the breach happened, whether and what specific information was compromised, and what mitigating measures might have been in place to minimize harm to individuals (such as encryption or key coding). Thus, the information available to the controllers, which would then be provided to the DPAs, would be insufficient for the DPAs to meaningfully evaluate the situation or make any kind of useful recommendation on the notice to individuals. Replacing the GDPR's "undue delay" requirement for processors with an "immediate" notice period is likely to result in processors and controllers erring on the side of caution and issuing notices to DPAs with incomplete information. DPAs will then be saddled with the burden of trying to figure out which notice reflects significant risk to individuals, which companies should be investigated, and where action by a DPA is warranted. Given the significant risk of failing to provide notice, responsible companies will be compelled to provide a notice breach prematurely and without an opportunity to investigate resulting in excessive over-notification to the DPAs.

In some cases, there may be very important reasons to delay provision of a notice. For example, consider a software provider that discovers that a backdoor on its software has been created by an intruder. If this were discovered by law enforcement, law enforcement would advise the service provider to delay informing its customers until it has had a chance to fix the vulnerability and push out the software patch to its customers. To give an immediate notice without an established fix would tip off the bad actor and create significant vulnerabilities for the organization's customers and the individuals who use platforms supported by that software (which could include government as well as private sector entities). The answer to that problem is not that the processor can give notice to the DPAs directly because the processor will have no knowledge of the data protection laws to which its customers are subject. As currently proposed by the Working Party, however, in that context the customer would be in violation of the GDPR despite the fact that it has no knowledge of the potential breach because its processor, for valid reasons, did not provide immediate notice.

Many companies elect to outsource some of their data processing to firms that can provide better security than the companies can themselves. Even assuming that the processor can manage to provide notice very quickly – it might still take more than 24 or 48 hours for the processor to inform all of its customers. Thus, if a customer is not notified within 48 hours of the processor becoming aware of the breach, that would mean that the controller then only has 24 hours to notify the DPAs. Imposing such short notification timeframes penalizes organizations that opt to outsource their data processing activities even if they are entirely without fault and have done everything properly.

Direct Liability of Processors. Unlike the Data Protection Directive, the GDPR imposes obligations on both controllers and processors. Controllers are required to use processors that provide sufficient guarantees to implement appropriate technical and organizational measures so that the processing will meet GDPR requirements. Such processing must be governed by a written contract that is binding on the processor and sets out the terms and conditions of the processing. Because processors are now directly subject to GDPR requirements, the DPAs have the ability to hold processors directly accountable. Thus, if a processor fails to give notice to the relevant controllers without undue delay, the DPAs can hold the processors directly accountable (without having to work through the controller). The GDPR provides remedies in the event that processors fail to adhere to their GDPR obligations.

Unfair Liability. It is unfair and unreasonable to assume that a controller is aware of a breach once the processor is reasonably certain that a personal data breach has occurred, regardless of whether or not the processor has informed the controller of this fact. If the controller has met its obligations under the GDPR, it has properly selected a processor, it has supervised the processor, and it has established appropriate contractual provisions, then it should not be liable for the misdeeds of its processors, particularly when it has no knowledge of the breach and no ability to take action. To do so would unfairly penalize the company even if it did everything right. The GDPR includes significant potential liability for controllers. The language of the GDPR states that the obligation to provide notice of a personal data breach arises 72 hours after the controller becomes aware of the breach. By imputing knowledge to the controllers, based on the processor becoming aware, the Working Party is in fact imposing a liability standard on controllers which is not found in the GDPR. For example, a controller can add contractual obligations requiring immediate notice. If the processor fails to live up to the contractual provision and gives the controller notice after 96 hours, there is nothing that the controller can do to remedy that violation. The controller would be in violation of the period imposed by the Guidelines without even being aware of it. This is inconsistent with the GDPR and with the Guidelines that focus on when a company is reasonably aware. The Guidelines seek to impute awareness when it may be impossible for the controller to in fact be aware.

In conclusion, when processing is being carried out by a third party processor and the processing is subject to a breach, we believe that the Guidelines should follow the "undue delay" notification approach for processors set forth in Article 33(2). There should be no attempt to impute the controller's awareness until such time when the processor has given notice to the controller.

Sincerely,

/S/

Miriam H. Wugmeister

cc: Cynthia Rich