GOOGLE FINED €50 MILLION BY FRENCH AUTHORITIES FOR GENERAL DATA PROTECTION REGULATION ("GDPR") VIOLATIONS

GDPR POST-EFFECTIVE DATE COMPLIANCE REQUIREMENTS

January 2019

I. Executive Summary.

On January 21, 2019, the French data privacy regulatory authority imposed a €50 million ($57 million) fine against Google for violations of the European Union's ("EU") General Data Protection Regulation ("GDPR"). The stated basis for the first GDPR fine was Google's failure to be clear and transparent in seeking consent and collecting data from users. The GDPR, which took effect on May 25, 2018 and which replaced and repealed the 1995 EU Data Privacy Directive, affects all persons, companies, and organizations, of whatever national domicile, that collect personal data on EU persons. The penalties for noncompliance can go to the higher of €20 million or 4% of the offender's global annual revenues, and the Google fine, taken with EU pronouncements, have made clear that the penalties are intended to have teeth, including against American companies. Moreover, the GDPR gives any person whose personal data is misused a private right of action for money damages and turns that person into a GDPR watchdog for penalties as well. Surveys indicate that up to 70% of U.S. companies have made no effort to comply with the GDPR, and the European Commission and European national regulators are expected to levy as much as $6 billion in fines in the first year or two of enforcement. For companies that have not addressed GDPR compliance, here is what you need to know and what you have to do.

II. GDPR Overview.

a. Controllers, Processors and Extraterritorial Effect. Any person or legal entity, wherever located, selling goods or services to, or monitoring the behavior of, natural persons in any of the 28 EU member states (called "Data Subjects" by the GDPR) is affected. The GDPR applies to both "Controllers" and "Processors," who are jointly and severally liable for data privacy breaches and compliance violations. Controllers are the persons or companies that determine the purposes, and means of the processing of personal data of Data Subjects; Processors are persons or companies that process the data on a Controller's behalf. Controllers and Processors must have GDPR-compliant written "Data Processing Agreements," or "DPAs," between them; their

requirements are discussed in section III (d). It is not yet clear to what extent, if any, sales of goods or services into the UK post-BREXIT will be affected, but the UK has indicated that it will enact a similar measure. So, for example, a US company selling goods or services into the EU, even remote "cloud" or hosting services, or even to EU citizens resident in the United States, is subject to GDPR enforcement.

b. Data Subject to Enforcement. The GDPR casts a much wider net in defining "Personal Data" subject to enforcement than many companies, particularly American companies, are used to respecting. The GDPR definition of Personal Data subject to enforcement includes anything that can be directly ***or indirectly*** used to identify a person. For example, Personal Data includes not only names, addresses, government-issued identification numbers, bank, and medical records, but also health, biometric or genetic data, e-mail addresses, social media posts, photographs, and computer IP addresses. In other words, any American website that accepts personal information from Data Subjects, or sends "cookies" to their IP addresses, is subject to GDPR enforcement. For all such Personal Data, a "reasonable" level of data protection must be provided to Data Subjects. However, what GDPR considers reasonable is extremely restrictive by American and other non-European standards.

c. Principles of Data Collection. The Controller is responsible for the collection and use of Personal Data. The following principles apply:

- Personal Data must be collected for specified, explicit and limited purposes and not processed for uses incompatible with those purposes once collected.
- Personal Data must be processed lawfully, fairly, and transparently.
- Personal Data must be maintained in accurate and up-to-date form, and data that is inaccurate must be erased or rectified without delay.
- Personal Data must be kept in a form that permits identification of Data Subjects for no longer than necessary for the purposes of data processing, and must be processed in a manner that ensures its security, to protect against unlawful or unauthorized processing, accidental loss, destruction or damage. (GDPR Art. 5).

d. Compliance Requirements. The gravamen of GDPR compliance for private companies and organizations is consent; clearly informed, unambiguous consent (GDPR Art. 6). "Opt-out" systems, especially beloved of American companies and which put an affirmative burden on the Data Subject, are unacceptable under GDPR; for sensitive Personal Data, only "opt-in" systems

will be compliant, in which the Data Subject must affirmatively agree to collection of his or her Personal Data; silence or non-action equals refusal to collection of data. For non-sensitive Personal Data, "unambiguous" consent will be sufficient, although there will in practice probably not be much daylight between that and full "opt-in" consent systems. Moreover, the request for consent and its purposes cannot be buried in legalese terms and conditions boilerplate (also beloved of American companies), but offered on a clearly understandable, readily accessible form. Whether for sensitive or non-sensitive Personal Data, the consent must be unambiguous (GDPR Art. 7). The purpose of the Personal Data gathering, storage, and/or processing must be attached to the form on which consent is given, and may not be exceeded in scope or in time; in other words, consent given for a specific, narrow purpose does not thereafter render the Personal Data generally available for the collecting company's use, resale, "data mining," or other purposes. Personal Data may not be stored for longer than the purpose for which consent was given, imposing on companies an affirmative obligation to purge already collected data. Consent may always be withdrawn, and the company collecting the Personal Data must make it as easy to withdraw consent as to give it (GDPR Art. 7). The Personal Data remains the property of the Data Subject giving consent, and any further, or extended, use of that data must be pursuant to a separately given consent. All of these standards are almost completely unknown and/or generally disregarded in pre-GDPR American business practice.

e. Penalties for Non-compliance. GDPR fines for noncompliance can go up to the ***higher of €20 million or 4% of the offender's global annual revenues***. The €50 million fine levied against Google, the first under GDPR, is obviously intended to make a statement: that those ceilings will be used in practice. The highest fines are expected to be imposed for the most serious violations, like violating Personal Data privacy without the Data Subject's consent. Within those limits, there is a second tiered level of fines for lesser breaches, such as not having records organized to the GDPR standard, or not notifying the GDPR regulatory authority of a data breach within the required 72 hours, for which fines may go up to the higher of €10 million or 2% of the offender's global annual revenues (GDPR Art. 83).

f. Private Right of Action. In addition to the above-stated penalties, the GDPR grants a private right of action to any Data Subject damaged by a Controller's or a Processor's infringement of the GDPR's standards (GDPR Art. 82). The private right of action is enormously significant, because it makes every Data Subject from whom Personal Data is collected a watchdog for abuses, who can not only seek damages in his or her own right, but refer the GDPR data breach

and the Controller or Processor at fault to the appropriate national regulatory authority for Art. 83 fines.

g. Special Rules for Children. Parental consent is required to process the data of children under the age of sixteen using online services offered directly to the child; individual EU member states may individually set the age as low as thirteen (GDPR Art. 8).

h. The "Right to be Forgotten." Under GDPR, Data Subjects may not only withdraw consent, but demand that information previously gathered be erased, which must be done, unless another legal requirement to retain records supersedes (GDPR Art. 17). This GDPR requirement is enormously at variance with American business practice, which traditionally treats data, once gathered, as its asset and property, and goes to enormous effort and expense not only to save and preserve it, but to "mine" it for inferable patterns and other information that can be exploited for business advantage, and is expected to be one of the most difficult areas of GDPR compliance.

III. Required Compliance Measures.

a. Appoint a Data Protection Officer ("DPO"). Companies or organizations that (a) are public authorities, (b) engage in large scale, systematic monitoring; or (c) organizations that engage in large scale processing of sensitive Personal Data must appoint DPO's (GDPR Art. 37). Companies or organizations not meeting those criteria need not appoint DPO's.

b. Conduct a Data Privacy Risk Assessment. The GDPR requires companies and organizations to audit their existing data privacy practices and third party contracts to assess what compliance measures are necessary. The audit, or risk assessment, should begin with "data flow mapping" to map the entire route of Personal Data entering the company or organization from the point of collection, until the time it is stored, processed, disseminated, or finally disposed of – where "it comes to rest" within the company. The types of Personal Data in the map should be assessed, including as to whether any children Personal Data is involved, for which parental consent may be necessary. All software and software applications that collect and store personal data must be included along with vetting of personnel having access to the data, a process that GDPR Art. 30 calls the "Record of Processing Activities." The risk assessment should review all Controller – Processor relationships and determine whether the required written Data Processing Agreements are in place and are GDPR compliant (see subsection "d" below) (Controller – Controller written

agreements are also required). The audit should further assess whether at any point in its travel through the company, the collected Personal Data can be used, misused, appropriated, disseminated, etc. for any purposes other than the specific one for which consent was given. Audit design itself must be customized to the size, scope, and activities of the company or organization.

c. Implement Remediation Measures Dictated by the Audit. Virtually no American company or organization that, for example, takes website orders directly, or processes data for others, will be GDPR-compliant, except in the unlikely case that no such data from EU citizens is accessed. Most American websites have exactly the kind of "legalese," boilerplate terms and conditions that the GDPR forbids and that European authorities intend to sanction with fines, and do not have simple limited consent and withdrawal-of-consent forms. Most American companies and organization are accustomed to keep collected data forever, and to use it for purposes other than that for which it was given.

That all must change. All Data Subject customers must be informed of their GDPR rights. All Personal Data must be collected, processed, and maintained in such a way that it is not used for purposes and time greater than that for which consent to collect it was given. All Controller companies or organizations that have outsourcing relationships with third party Processors for data storage, processing, or other related services (for example, cloud storage providers, billing and payroll services, payment portals, and others) must enter into or review Data Processing Agreements, or DPAs, contracts with those third party Processors and ensure that the Processors are also in compliance, and that the DPA contracts between them provide for GDPR-standard data management and protection compliance and breach notification since, under the GPDR. Controllers are responsible for their Processors (for more detailed treatment of the Controller – Processor relationship and DPAs, see subsection (d) below).

Internal controls will have to be established as a result of the company's risk assessment. For example, data entry personnel will need a set of protocols governing their collection and input of Personal Data, and to make sure that they do not disseminate the Personal Data collected and processed for any use other than the one for which consent was given. Similarly, the personnel actually working with the Personal Data will need a protocol limiting their use of it strictly to the one for which consent was given, and for disposing of, or securing, it once the use for which consent was given is ended.

Protocols for disposal of Personal Data no longer used for the purposes for which consent was given, and for withdrawal of consent/"right to be forgotten" cases must also be put in place. Ongoing periodic compliance audits must be established. The company or organization should also test its protocols by putting a test data breach into its systems where risk has been identified. Risk containment, remediation, and breach notification can thereby be tested.

d. Controller – Processor Relationships and Data Processing Agreements. As between all Controllers and Processors, written Data Processing Agreements, or DPAs, providing for GDPR compliance must be entered into, maintained, and complied with. GDPR Art. 28 – 36 set out a non-exclusive list of issues that must be addressed in all DPAs, including:

- The DPA must set forth the subject matter of the Personal Data processing, its duration, the nature and purpose of the processing, the types of Personal Data involved, any special categories of data involved; and the Controller's and Processor's rights and obligations.
- The DPA must have appropriate confidentiality provisions, including for downstream "sub Processors" subcontracted to by the Processor.
- The DPA must provide that the Processor must have the Controller's consent to use sub Processors, manage its sub Processors, and ensure that sub Processors adhere to the same standards the Processor adheres to in direct processing for the Controller.
- The DPA must provide that the Controller and the Processor must have adequate information security in place.
- The DPA must provide covenants and procedures for the Controller and the Processor to cooperate with the Controller on any data protection regulatory authority investigation.
- The DPA must provide for the Processor to notify the Controller of any Personal Data breaches without delay and for the Controller to report Personal Data breaches to the appropriate regulatory authority within 72 hours.
- The Controller and the Processor may have to appoint a DPO.
- The Controller and the Processor must keep records of all processing activities.
- The Controller and the Processor must comply with EU trans-border data transfer rules.
- The DPA must have provisions to obligate the Processor to assist the Controller to comply with Data Subjects' rights.
- The DPA must have appropriate (for the context) representations, warranties, covenants, indemnities, and other provisions to be expected in such an agreement.
- The Processor must assist the Controller in managing the consequences of Personal Data breaches.

- The DPA must provide for procedures to destroy or return Personal Data at the end of the agreement's term or upon a Data Subject's request. The Controller must, in addition to assuring that a compliant DPA is in place with all Processors it uses, assure and provide evidence of its due diligence in engaging a qualified Processor in terms of the types of personal data to be processed.

The GDPR represents an enormous challenge to American companies, given their traditional practice of treating Personal Data, once obtained, as their property to data mine, analyze for purposes other than that for which the data was originally obtained, and exploit for commercial advantage in perpetuity. The French Google fine makes clear that the challenge is now at hand, and while compliance will be burdensome and inconvenient, and may be the subject of lobbying efforts and court challenges in the U.S., the more restrictive standards for use of Personal Data set by the GDPR for Europeans are likely to increasingly become the expectation of American consumers. Under the circumstances of the GDPR, with the new GDPR-like California Consumer Privacy Act scheduled to come into force in 2020, and with a renewed consumer interest in data privacy as a result of serial data breaches at major corporations, revelations about Facebook's and other social media sites' data practices, and political news reigniting consumer awareness of and interest in data privacy, it is good sense to avoid ruinous fines and adopt stringent data collection and processing practices to the GDPR standard and turn them into a competitive advantage. Despite some arrogant pronouncements in years past, privacy turns out not to be dead after all.

Owen D. Kurtin