GLADE VOOGT LORD SMITH PC™

Law Update for Clients

Is Your Business Ready to Comply with the New Requirements of the European Union's General Data Protection Regulation?

The new privacy law is effective as of May 25, 2018 –and there is not much time left to prepare

By David Aschkinasi

Special Counsel – Glade, Voogt, Lord & Smith, PC

With the recent massive theft of confidential information of almost 150 million people from the credit evaluator Equifax' databases, any business that handles personal information is now on notice that it must exercise diligence in protecting the personal data of customers, vendors and service providers. It now appears that the Equifax breach could have been prevented if Equifax had a process in place that assured that when weaknesses in its operational security were identified, responses and fixes were immediately implemented. Equifax was aware of the software flaw that allowed the security breach, and it was also aware that a patch, or fix, for the problem was available. Unfortunately for many millions of Americans, Equifax did nothing to fix the problem, before hackers infiltrated their systems and stole the names, addresses, social security numbers, birthdates and financial information of almost half of the American population.

The Equifax story will resonate with government regulators and with the public, and should serve as a warning to businesses that they must have processes in place that will identify risks and weaknesses in their systems that maintain personal and confidential information. Businesses will likely be held to a higher standard of care for their actions or failures to act to protect that information. With all the publicity regarding the Equifax breach, it will be almost impossible for a company to claim ignorance of the risks of cyber-attacks and the need for processes to protect themselves from such risks. Businesses must establish or review existing processes for cyber-protection to minimize the risks of being hacked. They must also establish processes to assure that third-parties that possess confidential information on behalf of the business comply with all applicable laws, and that those third-parties have processes in place to assure the safe-keeping of that information. The first steps that businesses must take are to determine the type of personal data that they possess, and then evaluate how well protected that data is from unauthorized release.

As U.S. businesses focus more and more on global markets and a global customer base, they must understand that whatever practices and procedures they may have in place to assure the security of their networks and data may also have to comply with the stringent privacy and data protection rules of the European Union (EU). A U.S business that has operations, customers, or service providers in the EU, or processes personal information related to EU residents must analyze its operations to determine if it

complies with the EU laws as well as any U.S. or other applicable privacy or data protection laws.

The EU adopted a new privacy and data rights law, the General Data Protection Regulation (GDPR), that becomes effective on May 25, 2018. The GDPR reinforces the existing rights of individuals under the current EU Privacy Directive, and provides new protections and rights to individuals to better protect their personal data. The GDPR will apply to all companies operating in the European Union, as well as to any company that processes the personal data of people located in the EU countries. The law will apply to companies that process data relating to the offering of goods and services to people in the EU as well to the monitoring of those people's behavior. Over the next several months, the various data protection officials in the EU member states will likely issue additional guidance or regulations that relate to interpretation and enforcement of the GDPR.

To understand if a company's existing processes for data protection meet the new EU requirements, a compliance review should be undertaken to analyze what data it holds or processes, how that data is protected, what risks exist related to the inadvertent release or malicious theft of that information, and whether its existing processes comply with new GDPR requirements.

Does the GDPR apply to your business?

- If your business is established in any EU member state, the GDPR will apply.
- If your business is outside of the EU, but is a data controller or processor, and offers goods or services in the EU or monitors behaviors of data subjects in the EU, then the business is subject to the provisions of the GDPR.
- If any of your vendors or service providers collect or process the personal information of EU residents on behalf of your company.

It will be helpful to know the definitions of a few terms frequently used in the GDPR:

Data Subject – an identified or identifiable natural person

Personal Data – any information relating to an identified or identifiable natural person (data subject)

Processing – any operation or set of operations which is performed on personal data such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

Profiling – any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Consent – any freely given specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Impact Assessment (DPIA) – Article 35 of the GDPR requires that data controllers conduct an analysis to determine the impact that planned processing may have on the protection of personal data, such requirement depending on the scope of processing and risk that the processing creates to the rights of natural persons.

Cross-Border Processing – processing of personal data which takes place in the context of the activities of establishments in more than one EU member country, or which substantially affects or is likely to substantially affect data subjects in more than one EU country.

What are the Rights of Data Subjects under the GDPR?

- The right to receive information from data controllers stating the identity of the controller, contact information for the controller, the purpose and legal basis for the processing of personal data, and any intended cross-border transfers of personal data.
- The right to obtain confirmation from the controller that information is being processed, and to have access to the data and to receive a copy of the data processed.
- The right to correct data that is incorrect or incomplete.
- The right to erasure, also called "the right to be forgotten" is the right to be removed from databases.
- The right to transfer personal data to another data controller (data portability).
- The right to restrict the processing of data, if the data is inaccurate, if the processing is not legal, or if the controller no longer needs the data for the intended processing.
- The right to object to processing if the basis for the processing is that it is in the public interest or in the interest of the data controller.
- The right not to be subject to a decision based solely on automated processing or profiling, or which produces legal effects concerning the data subject or significantly affects the data subject.
- The right to withdraw consent to processing at any time, in a manner as easy as it was given.

What are the Obligations of Data Controllers?

- Provide information to data subjects and communicate with them in response to their legitimate requests in a concise, transparent and easily accessible manner.
- To respond without undue delay at least within one month after receiving a request
- To implement appropriate data protection policies
- If processing is to be performed by a separate data Processor, the Controller must enter into a written agreement with the Processor including the following provisions:
    - Specific instructions regarding processing, including instructions related to any transfers of personal data a 3rd country or an international organization
    - Processors shall commit to confidentiality of personal data
    - Processors shall commit to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.
    - Processors shall not engage another processor without consent of the Controller, and any such engagement will be pursuant to specific contractual commitments.
    - Shall assist the Controller in complying its obligations to maintain secure conditions to protect the confidentiality of the data.
    - Shall return or delete all personal data, at the direction of the Controller, after the processing has been accomplished.
    - Shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and shall allow for and contribute to audits or inspections by the Controller or its designee.
- To have processes in place for new and existing products and services that ensure that only personal data which are necessary for the specific processing are processed (Privacy by Design).

What are the Obligations of Data Processors?

- Data Processors must operate in a manner that assures having technical and organizational measures in place to assure that it will comply with all requirements of the GDPR to protect the rights of data subjects.
- All processing by a Processor must be carried out under a binding contract that described the subject-matter, duration of the processing, the nature and purpose of the processing and the types of personal data and categories of data subjects who data will be handled. Only processing that is described in the agreement

between the Controller and the Processor may be undertaken.
- Processors may not engage other processors without the written instructions and consent of the Controller.
- Processors must maintain a record of all categories of processing activities carried out on behalf of a Controller, and those records are subject to review by the Controller and any supervisory authority.

Potential Liabilities for Violations of the Rights of Data Subjects:

- Both administrative and judicial remedies may be available for claims against controllers and processors
- Compensation may be available for material or non-material damage suffered by a data subject as a result of a violation of the GDPR.
- Administrative fines for violations are authorized for up to EUR 20 million (US$23.5 million) or 4% of the worldwide annual turnover of the preceding fiscal year, whichever is higher

A Data Protection Impact Assessment (DPIA) is a Critical Tool to Evaluate Compliance with the GDPR:

- Article 35 of the GDPR states that a DPIA is required where processing activity is likely to result in a high risk to the rights and freedoms of natural persons.
- Although some examples of high risk situations are provided in the GDPR, the Article 29 Working Group of the EU, whose members represent the data protection authorities of each of the EU member countries, states: "DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing… Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance." Regardless of whether a DPIA is mandatory, a DPIA is strongly recommended, based on the Article 29 Working Group's guidance.
- The GDPR states that it is the "risk to the rights and freedoms of natural persons…(that) may result from personal data processing" that is of concern, not a risk to businesses.
- A DPIA should include the following:
    - A description of the processing operations and the purposes of the processing, including whether the processing is necessary to achieve the purposes
    - An evaluation of the risks to the rights of data subjects
    - How the risks will be addressed, including organizational and technical processes, physical and logical security

Is Your Business Ready to Comply?

- Have you conducted a survey to determine if your business is subject to the GDPR, and if so, is your business a Controller or Processor of personal data?
- Do your employees, managers, and board members understand the GDPR, the rights it grants to data subjects, and the obligations placed on data Controllers and Processors?
- Are your data storage and data processing systems secure, in compliance with the requirements of the GDPR?
- Do you understand the legal basis on which you use personal data?
- Do you have clear policies in place to show that you meet the required standards?
- Do your policies or organizational structure create a system of accountability for compliance?
- Do you have adequate training to assure that employees and managers understand their responsibilities?
- Do you have a system in place to receive, track and respond to the requests of data subjects?
- Do your agreements with customers, service vendors, and suppliers have adequate provisions to show consent to collect and process personal data, to protect personal data and to otherwise require compliance with the GDPR?
- Is your business ready to be audited for compliance with the GDPR and any contractual commitments related to the protection and processing of personal data?
- Is your business and its employees and managers aware of the risks associated with non-compliance?
- Does your business incorporate into the process for developing new products and services, or for reviewing existing products and services, measures that ensure that only personal data which are necessary for specific purposes are processed?

Conclusion:

All businesses should hear the message that they should develop an understanding of all applicable privacy and data protection laws, especially those in the EU, and evaluate whether they comply with those laws. A compliance review and adequate compliance program are essential to comply with the obligations to protect personal data and to prevent data breaches. Appropriate compliance programs will also lower business risks associated with potential data breaches.