GENERAL DATA PROTECTION REGULATION
MAY 2018

Virginia Economic Development Partnership Global Network

This information is being provided at the request of the VEDP. Any information provided or reference to any specific product, service, business, firm or corporation is provided solely for informational purposes only and does not constitute an endorsement or recommendation by the State of Virginia, the Department, or its officers, employees, or agents. The information does not constitute legal or financial advice, nor is it an assurance, guarantee or warranty of the accuracy, completeness, or usefulness of the information. The State of Virginia, the Department and its employees or agents shall not be liable for any damages arising from the use of or reliance on the information.

IBDG

International Business Development Group

March 2018

Virginia loves Exports
CONTENTS

GENERAL DATA PROTECTION REGULATION .................................................................................................................. 1

1.0 WHAT IS GDPR? ....................................................................................................................................................... 1

   1.1 SCOPE OF THE GDPR ............................................................................................................................................... 2

   1.1.1 U.S. COMPANIES THAT ALREADY HAVE A PRESENCE IN THE EU ............................................................... 2

   1.2 U.S. COMPANIES WITHOUT A PHYSICAL PRESENCE IN THE EU BUT DEALING WITH EU RESIDENTS AND CITIZENS ................................................................................................................................. 2

2.0 KEY ELEMENTS OF GDPR ........................................................................................................................................ 2

   2.1 A PERSON'S CONSENT ............................................................................................................................................... 2

   2.2 TRACKING AN INDIVIDUAL IN THE DIGITAL WORLD ............................................................................................ 2

   2.3 THE RIGHTS OF THE INDIVIDUAL TO CONTROL THE USE OF THEIR PERSONAL DATA ...................................... 3

   2.4 PRIVACY MANAGEMENT ......................................................................................................................................... 3

3.0 COMPLIANCE ............................................................................................................................................................... 3

   3.1 FAILURE TO COMPLY ............................................................................................................................................... 3

   3.1.1 WHAT IS THE DIFFERENCE BETWEEN A DATA PROCESSOR AND A DATA CONTROLLER? ......................... 3

   3.2 DATA BREACH NOTIFICATION REQUIREMENTS ...................................................................................................... 3

   3.3 NOTIFICATION PROCESS ......................................................................................................................................... 4

   3.4 PROOF OF COMPLIANCE ........................................................................................................................................ 4

   3.5 DOES MY BUSINESS NEED TO APPOINT A DATA PROTECTION OFFICER (DPO)? .................................................. 4

ADDITIONAL RESOURCES ............................................................................................................................................... 4
GENERAL DATA PROTECTION REGULATION

“In the EU, privacy is a right; in the US, it is a commodity”
Peter Milla, Data Protection Officer at Cint. https://www.cint.com/

The following information is a brief summary only of the new GDPR regulation coming into force in Europe. An in-depth review should be undertaken or legal advice sought by US companies that will need to comply with this new ruling.

1.0 WHAT IS GDPR?

The European Union’s General Data Protection Regulation (GDPR) comes into effect in May this year and replaces the 1995 Data Protection Directive.

As of May 25, 2018, all companies that have operations in the European Union (EU), offer goods or services to EU residents, or monitor or profile EU residents e.g. through online behavioral advertising, will be required to comply with the new GDPR.

GDPR’s main aim is to protect the personal data of EU citizens. This refers to how the data is collected, stored, processed and even destroyed. The full extent of the term “personal data” needs to be examined in greater detail because it exceeds the scope of how similar terms are defined in the U.S.

Under the GDPR, “personal data” means information relating to an identified or identifiable natural person, and a person’s “identifiers” can be obtained from a variety of information sources. Here are some of the main identifiers but not a complete list:

» A person’s name
» Their identification numbers e.g. social security, national insurance or passport
» Any form of economic and financial data e.g. bank details, credit cards, debit cards, etc.
» Their social media and online data including IP addresses, social media posts, online contacts and mobile devices
» Their location data, which is a common feature of some mobile apps
» A person’s race or religious affiliation
» Health and genetic data

This is not a complete list, so a more in-depth study of the new regulation will need to be undertaken by your company to ensure that what constitutes a person’s identifiers are fully understood.
1.1 SCOPE OF THE GDPR

The GDPR covers companies operating within and outside the EU. This means, therefore, that any company dealing with the EU commercially, academically, scientifically, medically, or in any capacity that accesses and holds EU citizens’ data, will have to comply with the GDPR. Even if a company does not have a European presence, it will still have to understand the impact of GDPR if it processes any data in connection with goods and services offered to an EU resident.

1.1.1 U.S. COMPANIES THAT ALREADY HAVE A PRESENCE IN THE EU

U.S. companies that currently have a physical presence in the EU are already bound by the EU’s current Data Protection Directive, which is being replaced by the GDPR in May 2018, so they will be used to operating under EU data privacy law and understand the legal and cultural differences between the U.S. and EU approaches to privacy. They will also be familiar with the new requirements and the consequences of non-compliance.

1.2 U.S. COMPANIES WITHOUT A PHYSICAL PRESENCE IN THE EU BUT DEALING WITH EU RESIDENTS AND CITIZENS

The situation is more complicated for U.S. companies that offer goods and services to EU residents but that do not have a physical footprint in the EU. Under current EU legislation U.S. companies have been able to transfer personal data from the EU to the U.S. lawfully. This is because the existing EU Directive in force today does not impose requirements on U.S. companies that do not have physical operations there. This will now change in a number of important ways. The GDPR will retain restrictions on cross-border transfers to countries that the EU believes do not provide adequate data protection.

2.0 KEY ELEMENTS OF GDPR

2.1 A PERSON’S CONSENT

One of the main considerations for all US companies dealing with the EU will be the GDPR’s requirement to obtain freely provided, specific, informed, and unambiguous consent before collecting personal data (i.e. information relating to an identified or an identifiable natural person, including a unique device ID or location data) from an EU resident. Obtaining an individual’s consent is a basis for legal processing and such consent should be demonstrable – organizations need to be able to show clearly how consent was gained and when. An individual’s silence, inactivity, or failure to uncheck a pre-checked box will not indicate consent. Companies that do not obtain consent to collect personal data must have another valid legal basis or legitimate interest (defined in the GDPR) for doing so, e.g. for the necessary execution of a contract. This is why it is going to be extremely important and necessary to examine the details of the GDPR more closely and with proper legal understanding. Something that might not be obvious, for example, is that GDPR will apply to non-EU data processors. This includes cloud service providers storing or hosting the personal information of EU data subjects.

2.2 TRACKING AN INDIVIDUAL IN THE DIGITAL WORLD

One of the GDPR guidance notes, for example, defines this as the situation when individuals are tracked on the Internet. This includes the potential use of profiling techniques to make decisions about the data subject, or for analyzing or predicting personal preferences, behavior and attitudes. This can be connected to a person’s shopping habits, purchasing history, eating preferences, etc.
2.3 THE RIGHTS OF THE INDIVIDUAL TO CONTROL THE USE OF THEIR PERSONAL DATA

The GDPR will give EU residents certain rights, such as the right to request removal of personal data that they have posted online and the right to data transferability. For example, a company will be required to remove, erase, or completely delete the personal data of an EU resident upon request. This could arise in situations where the data held is no longer necessary for the purpose for which it was originally collected, or the EU resident withdraws consent or objects to the processing of the data. In addition, a company will have to, at an EU resident’s request, transfer that resident’s personal data in a structured, machine-readable format to another company. U.S. companies will have to build this functionality into their systems and databases.

2.4 PRIVACY MANAGEMENT

Organizations will need to review their data protection safeguards. The GDPR mandates a ‘Risk Based Approach’ where appropriate organizations’ controls must be developed according to the degree of risk associated with the processing activities. Data protection safeguards must be designed into products and services from the earliest stage of development and any privacy-friendly techniques will be encouraged (e.g. pseudonymisation). There will be an increased emphasis on record-keeping in order to improve the capabilities of organizations to manage privacy and data effectively. However, this requirement will be less important where data processing is not a significant risk, particularly for small businesses (less than 250 staff).

3.0 COMPLIANCE

3.1 FAILURE TO COMPLY

Failure to comply with the new regulation includes fines of up to 4% of corporate annual turnover or a maximum of €20 million. This includes both controllers and processors of personal data, so companies holding or controlling a person’s data, but which use a third party or outsourced solution to process a person’s data, are equally responsible.

3.1.1 WHAT IS THE DIFFERENCE BETWEEN A DATA PROCESSOR AND A DATA CONTROLLER?

A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity which processes personal data on behalf of the controller.

3.2 DATA BREACH NOTIFICATION REQUIREMENTS

Companies that experience a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data will be required, subject to some exceptions, to notify:

» The relevant Data Protection Supervisory Authority in the relevant EU Member State where the person resides “without undue delay and, where feasible, not later than 72 hours after having become aware of it.” However, GDPR takes into account the fact that some companies may not know or be able to evaluate the seriousness of a data breach within 72 hours of detecting it, so it does allow for information to be provided in phases.

» Any individual whose data is at risk as a result of the data breach and that is likely to result in a high risk to the rights and freedoms of individuals. In the U.S., data breach notification is governed by 48 different state laws, none of which imposes such a short time period within which notification must be made because it often takes more than three days to determine the nature and scope of a breach.
3.3 NOTIFICATION PROCESS
EU data-breach letters must specify the nature of the data categories compromised, the number of data subjects affected, the name of the company’s data protection officer (DPO), contact information for individuals to learn further information, likely consequences for the data subjects, and measures taken to reduce risk to individuals.

3.4 PROOF OF COMPLIANCE
The GDPR will require companies to maintain records of all processing of personal data. Companies will need to turn records over to Data Protection Authorities, when requested, to verify compliance. Failure to do so could be subject to the fines mentioned above. U.S. companies will need to put in place appropriate technical measures to ensure compliance with these requirements.

3.5 DOES MY BUSINESS NEED TO APPOINT A DATA PROTECTION OFFICER (DPO)?
DPOs must be appointed in the case of:
» Public authorities
» Organizations that engage in large scale systematic monitoring
» Organizations that engage in large scale processing of sensitive personal data

ADDITIONAL RESOURCES
» Download the full GDPR details and learn more here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/