{W} WAKEFLY | *BEYOND EXPECTATION*

Bringing digital marketing and
web technologies together to elevate
your brand online

The Marketer's Guide to GDPR

(General Data Protection Regulation)

WAKEFLY, INC. | Wakefly.com | 508-616-2042

INTRODUCTION

In today's technologically advanced world, personal data transfer is occurring all the time. You cannot rent a car, make a purchase from Amazon, check your bank account, use Google Maps or visit a website without exchanging your personal information. While we all enjoy the conveniences of using modern technology, there are associated risks and we trust that companies will handle our personal information with great responsibility, collecting it only for their intended purposes of conducting business.

As global markets continue to expand and the demand for personal information increases, governments all over the world have proposed legislation that attempts to provide citizens with a standard of protection that promotes the free exchange of goods and services. Times change and with advancing technology, what was considered satisfactory 10 years ago could be a serious security issue today. To protect its citizens, governments must constantly review and amend legislation to make sure present concerns are addressed and work together to ensure a safe and secure global economy.

All companies that capture information from EU citizens, regardless of where the company is based or where the user is, are required to follow GDPR.

Two years ago, the European Parliament took its next step in data protection regulation by passing the GDPR. The GDPR not only resets the data protection standards for all European companies but now affects any country (particularly the United States) that conducts business with the European Union.

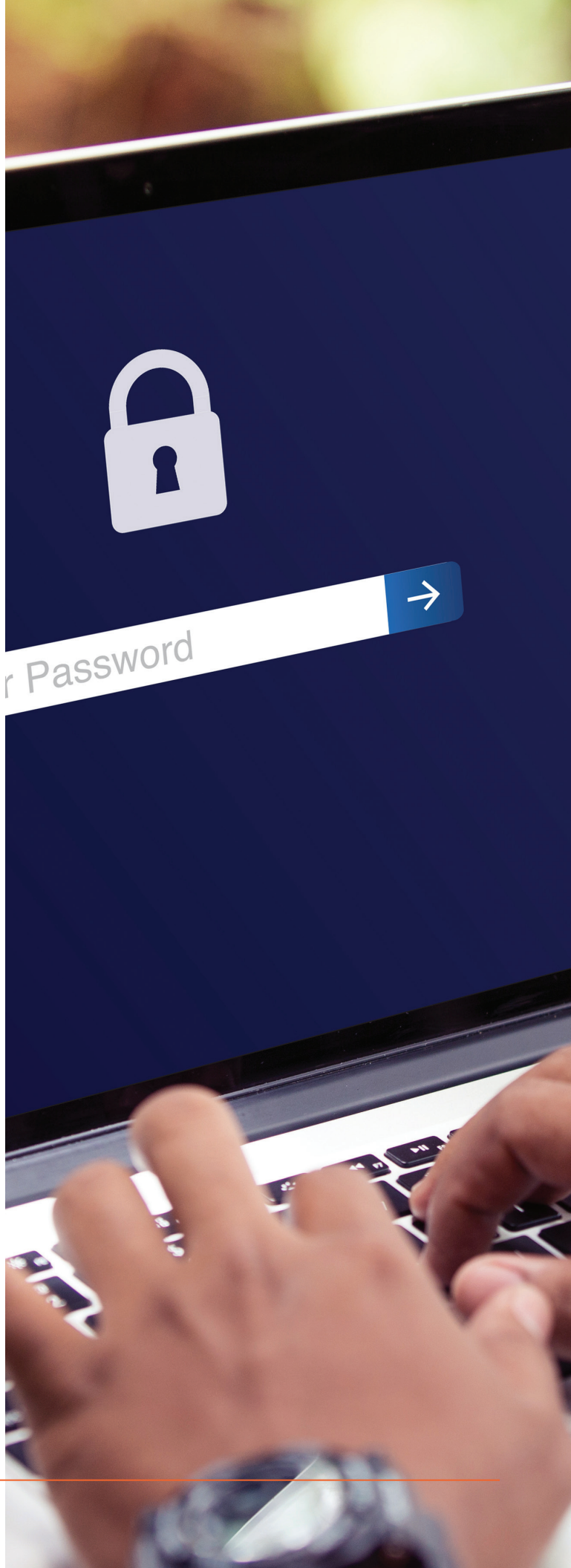
The General Data Protection Regulation (GDPR)

Since the 1980s The European Union (EU) has taken personal data protection very seriously. The EU's latest protective measure was passed in April 2016 titled the "General Data Protection Regulation", or commonly referred to as the "GDPR". Similar to the 1995 Directive, the GDPR is based on the "8 Principles of Personal Data" and its main objectives are to unify data protection laws across the EU, mandate similar requirements for non-EU countries and account for the current technology environment.

The GDPR replaces the "1995 Data Protection Directive" and continues the EU's longstanding data protection objective.

Notable additions include:

- Expanding on the definition of personal data
- Extending scope of jurisdiction (non-EU countries)
- Age of consent (children)
- The right to be forgotten
- Data portability
- Data breach notification
- Privacy by design
- One-stop-shop
- Unifying EU states providing greater coordination and consistency



WHAT IS GDPR?

Approved on May 24th, 2016, the GDPR was specifically designed to address the data protection challenges posed from technology advancements, unify EU member state laws and expand its scope to cover non-EU countries. Think of GDPR as a data protection sequel that kept true to the principles of the OECD guidelines and preceding directive storyline.

GDPR begins May 25th, 2018

The GDPR enforcement will begin effective May 25th, 2018 so it is imperative that companies from all over the world, who wish to conduct business or collect data from EU citizens, obtain compliance in accordance with the GDPR or be prepared to pay heavy penalties.

WHAT SPECIFIC CHANGES DOES GDPR BRING?

The GDPR includes several important variances from the previous directive aimed at enhancing the current EU data protection and privacy rights and protecting EU citizens from data breaches. These important changes include:

1. Increased Territorial Scope

Previously, EU laws did not apply to companies residing outside of the EU. Now, under the GDPR, protection extends its reach to include any company from any country (inside or outside the EU) that either conducts business or monitors the behavior of EU individuals. In other words, if you take data from an EU citizen, you must comply with the GDPR, regardless of your legal establishment. This includes businesses that collect data for mobile apps that track location or an international website that collects IP addresses or cookies. Additionally, businesses that operate outside the EU must select a representative in the EU that is responsible for responding to any questions or issues should they arise.

**Exceptions to this rule include:

- Non EU member countries that provide an adequate level of data protection and companies that employ fewer than 250 employees
- Non EU countries that conduct business or exchange data with EU individuals infrequently

2. Expand the Definition of Personal Data

According to Article 4 of the GDPR, personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person". This means that personal information is any information that can be traced back to an individual. Conversely, any data that cannot be traced back to an individual is considered anonymous and not considered personal data.
What defines personal data and the conditions that must be met to obtain compliance can be quite complicated and subject to change. This is why it is important to have a legal professional review the GDPR's definition of personal data and make sure you are in compliance with the definition. Even if requirements were fulfilled in the past, certain definitions may have changed. For example, the GDPR definition was recently expanded to include genetic data, health data and data for research. This type of data is considered "Sensitive Data" covered under Article 9.

3. Strengthened Consent Conditions

While consent for collecting or processing data was previously defined in the 1995 Directive, the conditions were enhanced to make the consent language as easy to understand as possible. Companies will no longer be able to require individuals to read long winded consent forms filled with complicated legalese terminology. All consent language must be clear and easy to understand. Additionally, if an individual wishes to "withdraw consent", they must be able to do so with no difficulty.

4. Privacy of Children and the Legal Age of Consent

It is important to note that Europe does not have child protection laws similar to the US COPPA online protection act. Additionally, the "age of consent" was not mentioned in the previous EU directive and was in desperate need of definition. The GDPR now addresses this issue and defines the legal age of consent of individuals to be 16 years of age. States however have the right to lower the age of consent to as low as 13 if they wish (Article 8).

Any person younger than 13 must have a parent or guardian grant consent to collect personal data when offering "Informational Services". Websites must provide clearly distinguishable consent forms when dealing with children.

5. The Right to be Forgotten

The right to be forgotten is discussed in Article 17 and sometimes referred to as "Data Erasure". This means that individuals who previously had their data collected or processed have the right to having it removed or erased at their request. For example, someone who used their credit card information to make an online purchase might want to make sure this information is removed from the site following a purchase. The data controller and any third parties who have access to this data are required to delete it upon request.

6. Data Portability

Under Article 18 of the regulation, a person has the right to request a copy of their personal information and have it saved in a common format (e.g. CSV file) in preparation to have it transferred to another controller, processor or service.

7. Privacy by Design

Article 23 covers the subject of privacy by design. Privacy by design means that data protection must be included within data systems from the beginning. Having data security should be at the forefront of any new data system, and in doing so, will help prevent data security issues such as data breaches. Security and privacy settings likewise should be set to high as a default. Article 23 also "calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing".

8. Data Breach Notification

This is one of the most important GDPR additions. If a data breach involving personal or identifiable data occurs, the supervisory authority and customers must be notified of the violation within 72 hours. If the supervisory authority feels that non-personal data is involved (e.g. unidentifiable or encrypted data), then customer notification is not required. Information that must be reported includes a description of the breach (categories, number of individuals affected and number of data records), contact information and recommended strategy to lessen the impact on customers.

9. One-Stop-Shop Solutions (OSS)

One-stop-shop solutions are designed to address the needs of data controllers who are established in more than one member state. Under the previous directive, data controllers who operated in more than one member state had to meet the unique data protection requirements of data protection supervisory authorities (SAs) of each state. Under the new GDPR legislation, the data controller now is only required to work with a single supervisory authority located in the member state of the company's main headquarters. This reduces the burden imposed on data controllers and provides consistency across the EU.

**Source EUGDPR.org

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Enforcement begins on May 25th, 2018. Since GDPR was approved in April 2016, companies have had 2 years to prepare.

Enforcement will be carried out between the combined efforts of both the supervisory authorities and the European courts and apply to both data controllers and processors. Reported incidents will be reviewed on an individual basis and if a violation has been committed, penalties of up to EUR 20 Million or 4% of annual global turnover (annual revenue), whichever is greater, will be given. Penalties will be based on a "tiered" basis according to the severity of the violation. "Intent" will play an important role in the assessment and final ruling. (Source EUGDPR.org)

How Does GDPR Affect US Businesses?

The passing of the GDPR in April 2016 has had a major effect on how US businesses handle personal data transferred between the EU. Previously, US companies were primarily concerned with US data protection rules and regulations. However, with GDPR enforcement scheduled to go into effect, there are additional international requirements to be concerned about. US companies that conduct business with European member states will not only have to review their current data collection process but also take a look at the data already in their possession, where that data resides and how that data is being distributed (e.g. third parties). US organizations must make sure their data collection process as a whole meets the rules established by the GDPR.

Please contact a GDPR compliance professional to ensure you meet all compliance requirements before the May 25th, 2018 deadline.

The GDPR is mainly concerned with personally identifiable information (PII); Examples of PII include name, address, credit card information, social security number, etc collected during an on-line business transaction or user session.

As a company, knowing the location of customer data is an important first step in determining if an issue exists. US businesses should also be aware that mobile apps are also covered under the GDPR and should be reviewed for risk potential. Encryption should be used whenever possible.

Cost and compliance complexities are other factors US companies should take into consideration. Depending upon the size of your organization and the amount of personal data you possess, the cost for full GDPR compliance can range anywhere from hundreds of thousands to millions of dollars. Because the financial burden incurred on US companies will differ, it is important to plan for GDPR compliance expenditures within your 2018 budget.

Due to increasing worldwide compliance regulations and advancing technologies, the pressures of meeting compliance standards have never been greater. Many IT departments will find it difficult to update their compliance standards and meet the May 25th deadline. A recent July 2017 survey conducted by Dimension Research, found that 61% of respondents have not even started. Some larger companies might find it worthwhile to hire a data privacy officer or utilize framework programs such as Privacy Shield to oversee their GDPR compliance process.

Finally, if a US based company cannot meet GDPR compliance or they find it financially impossible to do so, they may have to stop conducting business with the EU altogether. It is recommended that companies considering this option conduct a thorough cost-benefit analysis to help decide whether this is the best solution. However, most companies however are predicted to incur the cost of compliance.

WHAT STEPS SHOULD YOU TAKE TOWARDS GDPR COMPLIANCE?

****Note - This is a general overview meant for educational purposes only. Please contact a GDPR expert (data privacy officer) for detailed compliance recommendations.**

Since GDPR was approved in April 2016, companies have had 2 years to prepare.

- Start immediately – plan ahead and prepare for possible delays. Companies that have completed the process estimate 6 months.
- Become well versed in all GDPR rules or hire a data professional (e.g. data controller or data privacy officer) to help you through the process.
- Awareness – becoming aware of GDPR compliance standards is an important first step. Make sure you communicate this with all levels of management and IT divisions.
- Assess your current state of compliance health, taking note of every data storage location (e.g. third parties) and conduct a thorough audit noting your top areas of risk. Although this is an extremely time consuming task, leave nothing to chance. Assess the type of data you have, why you need it, where it is and how long you need it for.
- Delete any unnecessary data. Working from a smaller database can save you a great deal of time and expense.
- Locate the EU state you will be working in and contact your supervisory authority. Select a representative who will be the main point of contact for your organization.
- Make sure any new or future data processes have these regulations incorporated into the design. This includes any new technology purchases.
- Review your disclosure and consent forms. Make sure they are easy to read and understand. Also make sure it is easy for people to opt out.
- Make sure all third party sources are compliant. Remember you are responsible for everything.
- Make sure any new data collection follows GDPR guidelines.
- Utilize programs such as Privacy Shield or hire a data control officer to help you through the compliance process.

WEBSITE CHECKLIST FOR GDPR COMPLIANCE

****Note – This is a general overview meant for educational purposes only. Please contact a GDPR expert (data privacy officer) or utilize programs such as Privacy Shield for detailed compliance recommendations.**

- Make sure you have documentation on your website informing visitors that their information is being collected, the type of data being collected, why it's being collected, how long the information is being held for and a list of all protective security measures. This is typically continued in your online Privacy Policy or Terms of Use.
- Disclose any tracking cookies on your website and give people the option to opt-out without difficulty.
- Make sure you are aware of all types of personal data collected on your website. If you have any uncertainties, contact a GDPR professional to assist you.
- Make sure you are utilizing encryption as a part of your data collection and storage.
- Make sure all consent forms have an easy confirmation process (positive opt-in). For example, the option to click an approval button or check box. **Note- This must be separate from other terms and conditions.
- Make sure your privacy policy is up to date and a link provided within your homepage.
- If you have multiple privacy policies, make sure all links are provided on your website. Group them together for convenience.
- Make sure the contact information for all data privacy officers or data personnel is clearly listed on your website so inquiries or requests can be submitted.
- Make sure you have a process in place for easy data deletion (Right to be Forgotten).
- Make a list of all third party vendors and confirm the list is up to date. Check it often to make sure all vendors are accounted for and you know exactly where all data is going.
- Disclose any third party code on your website. Disclosure should be easy to locate and understand.
- Prepare for a data breach. Make sure you know who to contact in case of a data breach (e.g. supervisory authority, DPO, customers, etc.) and that all necessary forms are in place. Also make sure your communication process is set up efficiently and has the ability to contact all customers easily.
- Make sure all website security settings are automatically set to "high" as default.
- Be prepared for data portability requests. Make sure your data control process can easily convert an individual's personal data into a common format (e.g. CSV) and transfer to another service.
- Does your site deal with children? Make sure your legal age of consent privacy policy is up to date and clearly stated on your website (13 years of age in the US & UK while 16 in the EU).
- Does your company supply a mobile app? Review the data it collects, where it goes and the purposes it is collected for, and make sure it complies with the new GDPR.

****Reminder - Are you a large company (employing over 250 people) and collect/process large amounts of data on a frequent basis? Consider hiring a data privacy officer to oversee the entire compliance process.**

As a leader in bridging the gap between digital marketing and web development, Wakefly is ready to assist you & your development team on your journey to GDPR compliance.

Contact us today for a free consultation.