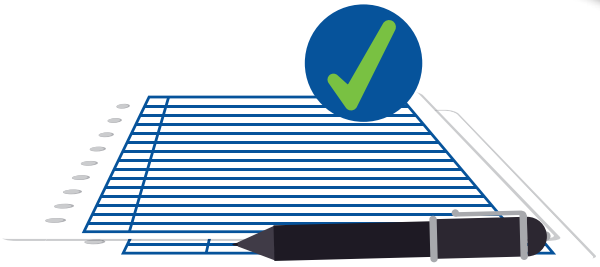
intelice SOLUTIONS

Your GDPR Quick-Start Guide

Are you behind the eight-ball when it comes to GDPR compliance? If you haven't finished your implementation, you are. The date to comply was May 25, 2018. The General Data Protection Regulation is a privacy law that the European Union is enforcing to protect the personal data businesses collect. Even if your business is outside of the EU, you must comply. We're providing our GDPR Quick-Start Guide to get you up to speed.



DISCLAIMER: We can't interpret the law for you; we're not lawyers. Please consult your legal advisor. The official document, in English, can be found here.

What is the GDPR?

The GDPR affects all internet business worldwide. It's a very complex law, so we can't explain everything here. We've provided some resources below that you should check out. Keep in mind that there are many gray areas where this law is concerned. So, you should do some research to determine how the law affects your organization's unique situation.

The GDPR is an internet privacy law. All businesses, small or large, and even entrepreneurs who do business on the Internet with consumers located in the European Union need to be aware of how the law affects them.

It doesn't matter if your company is inside the EU, or anywhere else in the world– If you do business with anyone in the following countries, you must comply with this new law by May 25th:

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czech Republic
7. Denmark
8. Estonia
9. Finland
10. France
11. Germany
12. Greece
13. Hungary
14. Ireland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Malta
20. Netherlands
21. Poland
22. Portugal
23. Romania
24. Slovakia
25. Slovenia
26. Spain
27. Sweden
28. United Kingdom

The GDPR is a consumer data protection law. It ensures that individuals can:

- Access their personal data.
- Export their personal data.
- Correct errors to their personal data.
- Object to the processing of their personal data.
- Erase their personal data.

The GDPR applies to the acquisition, processing, and storage of personal data – from initial gathering to final deletion of this data and every point in between. It applies specifically to personal data and anything that pertains to identifiable data such as:

Names
Email Addresses
Physical Addresses
Phone Numbers
Birthdate
Age
Sex
Race
ID Numbers
Nationality
Citizenship
Marital Status
Family Data
Health Data
Physical Characteristics
Profile Pictures
Occupation
Employment History
Income
IP Addresses
Cookies

(and more)

This could be information you collect automatically from Google, an opt-in, or other collection method online – anything that would identify an individual.

(301) 664-6800 • Info@Intelice.com

intelice SOLUTIONS

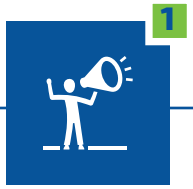
How Will The GDPR Affect My Business?

If your business has a website or an email list, you may be affected.

The GDPR affects any business relationship or transaction whether commercial or free where one or more of the entities are in the European Union. It's not based on citizenship, rather location. Any business within the EU must comply with the GDPR across its entire audience. If your business is in any of the 28 European Union Member States, you must comply with the law if you conduct a transaction with anyone located anywhere. If your business is located in the U.S. and you collect data about any business or person in the EU, you must comply with the GDPR.

How Should We Prepare For The GDPR?

There are three requirements you must meet.



Controls and Notifications

- Protect personal data using appropriate security.
- Notify authorities of personal data breaches.
- Obtain appropriate consents for processing data.
- Keep records detailing data processing.

Transparent Policies

- Provide clear notice of data collection.
- Outline processing purposes and use cases.
- Define data retention and deletion policies.

IT and Training

- Train privacy personnel and employees.
- Audit and update data policies.
- Employ a Data Protection Officer (if required).
- Create and manage compliant vendor contracts.

Some Examples

Before the GDPR:

Let's say you offer a whitepaper or free video to people online. Before the GDPR, your prospect provided their information, you gave them the freebie, and the consent was assumed because they accepted your gift. Pretty easy, right?

After the GDPR:

You can no longer assume that their consent is given if they accept your gift. Now you must specifically obtain their consent. It must be given freely, specifically, and be unambiguous. You cannot require users to give their consent to receive the gift.

> ***Note: This new standard applies to all of your existing lists. As of May 25, 2018, you can no longer send marketing emails to anyone who hasn't given their precise consent for you to keep their personal information. Plus, you cannot go back and ask them for their consent. You'll need a stand-alone system to do this.***

Compliance/Preservation

Step 1. Segment your email mailing lists into two parts.

- Non-EU subscribers
- EU-based subscribers and any unknowns

You want to continue to build goodwill with your Non-EU contacts, so reach out to them as you would have before. You will need to reengage with the EU-based and unknowns. Here's what we mean:

Step 2. Re-engage EU-based and Unknowns.

- Before emailing them, add additional value and content to your website.
- Then send them a link to your website and request their specific consent to keep their personal information.
- Set up a system to migrate those who give consent over to it.
- You must delete anyone in this group who hasn't consented.

Remember, storing and deleting their information is considered processing.

(301) 664-6800 • Info@Intelice.com

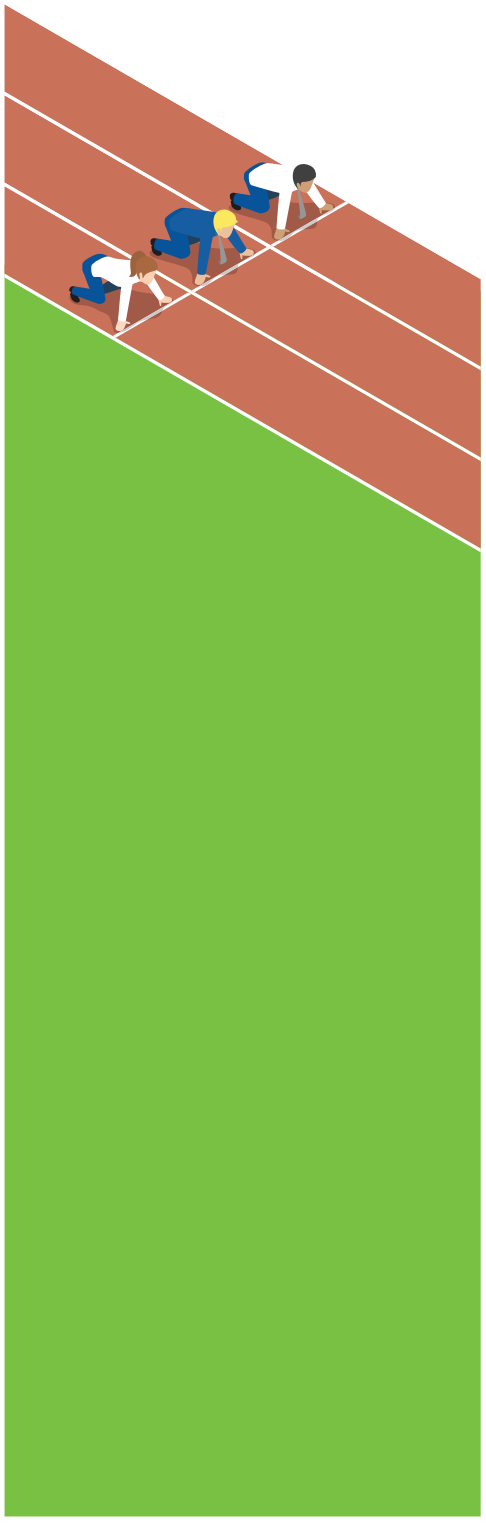
intelice SOLUTIONS

Breach Notification Requirements

The 2018 GDPR replaces the old Data Protection Directive of 1995. The most recent GDPR breach notification requirement was enacted in April 2016. It set a higher compliance standard for data inventory, and a defined risk management process and mandatory notification to data protection authorities.

Breach notification is a huge endeavor and requires involvement from everyone inside an organization. In-house tech support and outsourced Technology Service Providers should have acquired a good understanding of the consequences a data breach causes and the data breach notification requirements for their organization. They must be prepared in advance to respond to security incidents.

Get Your Quick-Start Advice Here



GDPR Compliance is complex, but at a very high level you need to consider the following:

Step 1: Do you have a lawful basis for processing personal data?

There are six available lawful bases for processing personal data. Which one(s) apply to you?

- Consent – Have you gotten specific consent from the individual?
- Contract – Do you have contractual obligations to process someone's personal data?
- Legal Obligation – Do you have a legal obligation to process someone's personal data?
- Vital Interests – Do you need to process someone's personal data to protect their life?
- Public Task – Are you a public authority or focused on public interest and need to process someone's personal data?
- Legitimate Interests – Do you have a compelling justification for your organization to process someone's personal data?

Step 2: Understanding the Individual's Rights

Data breaches and data misuse can greatly undermine an individual's right to privacy. GDPR provides individuals with the following rights. Each right has obligations which you must comply with.

- The right to be informed – Companies must provide certain information, like a privacy notice, and emphasize transparency over how companies use personal data.
- The right of access – Individuals will have the right to ask, and be responded to if an organization is processing their data. This information must be provided largely for free within one month of request.
- The right to rectification – If a person's data is incorrect or incomplete, he or she has the right to have it corrected. If you have given third parties that person's data, you must inform the person, and you must inform the third party of the correction.
- The right to erasure (be forgotten) – A person may request the removal of his or her personal data under specific circumstances.
- The right to restrict processing – Under certain circumstances, an individual can block the processing of their personal data.
- The right to data portability – A person can get their data for their own use any way they like.
- The right to object – A person can object to the use of their personal data for many purposes.

Step 3: Knowing what you must do to comply and the risks for not complying

Accountability, Governance, and Security are at the heart of GDPR. You are required to take the necessary steps to ensure the data entrusted to you is being managed appropriately. There are strict guidelines in how you must do so. In the event of a data breach, you must take the necessary steps to notify the authorities and individuals.

- Contracts – You need to have appropriate language in your contracts to ensure any processors are in compliance also.
- Documentation – You must document your processing activities.
- Data Protection by Design – You must design your processes and systems with individual data safeguards in mind.
- Data Protection Impact Assessments (DPIA) – You must perform a DPIA for any system which could result in a high risk to an individual's data.
- Data Protection Officers (DPO) – You must assign a DPO if you are a public authority or if your core activities include regular tracking of individuals, processing one of the special categories of data, or processing data related to criminal activities.
- Security – You must process data securely considering risk analysis, policies, physical, and technical measures. Your measures must ensure the confidentiality, integrity, and availability of the systems and services used to process personal data including recovering data if necessary.
- Personal data breaches – You must report certain data breaches to the relevant supervising authority usually within 72 hours. You must also notify individuals of any high-risk breach with undue delay.
- Failure to comply – If you fail to comply, you could be fined up to the greater of 4% of your worldwide annual revenues or 20 million Euros. You may also be banned from further processing.

In summary, all companies are required to comply with this regulation if they process any personal information regarding an individual from the EU. Even if you have a "Contact Us" form on your webpage, someone from the EU could submit their information to you, making it necessary for you to comply. You may believe that your risk is low or that the US will not allow any fines to be imposed on a US company. Regardless, we feel it's only good business practice to start heading in the direction of full compliance. Other governments are considering very similar regulations, so you may have to comply eventually with something similar.

The Following Are Additional Steps You Should Take To Prepare Your Technology

Your Technology Solutions Provider Can Help!

- Perform a thorough inventory of your personally identifiable information. Learn where it's stored–in onsite storage or in the Cloud. Determine in what geographical locations it's housed. Don't forget about your databases. PII is often stored in databases.
- Perform a Gap Analysis. This is a process where you compare your organization's IT performance to the expected requirements. It helps you understand if your technology and other resources are operating effectively. By doing this, your Technology Solutions Provider (TSP) can then create an action plan to fill in the gaps. The right TSP will understand the GDPR regulations and how your IT must support your compliance efforts.
- Develop an Action Plan. Your TSP should document a detailed action plan for how to use technology to meet the GDPR if you experience a data breach. This should include individuals' roles and responsibilities. Conduct tabletop exercises to practice how the plan will work with specific timelines and milestones.
- Ensure data privacy. If you don't have a Technology Solutions Provider, then you need one for this. Data protection is key for any-sized organization. Consumers have the right to have their data erased if they want. This is called "the right to be forgotten." This is a concept that was put into practice in the European Union in 2006, and it's a part of the GDPR. You won't be able to do this if their data is stolen.
- Be sure to document and monitor everything that you do that's related to GDPR Compliance. This includes any changes or upgrades that your Technology Partner makes to your IT environment. You may need to demonstrate that you've done your due diligence when it comes to protecting citizens' private information and that you practice "defense-in-depth" strategies where you use multiple layers of security controls when it comes to your technology.

Resources To Check Out For More Information

The European Commission's website regarding the GDPR:

https://ec.europa.eu/info/law/law-topic/data-protection

Wikipedia

General Data Protection Regulation

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Information from the service vendors you use:

- Mail Chimp
- Salesforce
- Google
- Microsoft

These and other services have GDPR-centric web pages with helpful information that impacts your relationship with them, how they handle processing, and how they can help you comply with the new regulations.

intelice SOLUTIONS

(301) 664-6800 • Info@Intelice.com