Article

General Data Protection Regulation (GDPR)

- Comply or Lose Out on Data Protection

Individuals across the Europen Union (EU) will now enjoy the privilege of advanced data protection and data privacy across Europe through General Data Protection Regulation (GDPR). The emphasis is on protecting citizens and their data and giving users more information about and control over how it's used. The new GDPR regulations will come into force from May 25th 2018.

National Governments need not pass legislative procedures as this is directly binding and applicable and effective from May 2018.

Organizations or businesses found non-compliant will face hefty penalties to the tune of up to 4% of their annual global turnover or €20 million, whichever is the highest.

What is GDPR?

GDPR requirement applies to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across the EU nations. Some of the key privacy and data protection requirement of the GDPR include

- Need the consent of subjects for data processing
- Anonymous data collection to protect privacy
- Provide data breach notifications
- Safely handle the transfer of data across borders
- Need certain companies to appoint a data protection officer to oversee GDPR compliance

Simply put, the GDPR mandates a baseline set of standards for companies that handle EU citizens data to better safeguard the processing and movement of citizens personal data. GDPR is a regulation which is a binding act and must be adhered to by all the EU members.

GAVS Technologies can help your customers be GDPR compliant and be conversant with what, how and when it's going to affect your business operations. We as a Solution Provider provide a communication platform to **Educate, Engage, Empower and Execute** (SAR) for Data Subjects and Data Protection Officers.

GAVS' GDPR platform uses the right mix of technology and processes to enable organizations quickly put in place a backbone for handling Data Subject Communications as well as empowering Data Protection Officers.

Built using the power of Office 365, Azure Cognitive Intelligence and other Microsoft Intelligent Cloud components, this platform is more than a compliance solution and can be extended to a CRM solution to help with organization's growth and improve the customer good will.

The platform along with the 4-step approach of **Educate, Engage, Execute and Empower** will help accelerate GDPR compliance for your organization.

Read on to know more about GDPR or attend our Webinar on "Enable the Rights of Your Data Subjects as Part of the GDPR Compliance" on Thursday, April 12, 2018, at 11:00 AM – 12:00 PM EDT.

The webinar explains the handling of new Access Requests without investing on new hardware, software and systems on premise and can be fully managed in Cloud.

If you're interested to know more about how GDPR affects your customer data, then contact us today at https://www.gavstech.com/reaching-us/

So, What Qualifies As "Personal Data"?

Any information related to a person or 'Data Subject', which can be used to identify the person directly or indirectly is classified as personal data. It can be anything from a name, a photo, an email address, bank details, social media posts, medical information, web data such as computer IP address, location, cookie data and RFID tags.

Who is Going to Be Responsible for enforcing Compliance?

The next question companies should ask is who is going to take responsibility for this activity? GDPR define several roles that handle compliance.

- Data Controller – Defines how personal data is processed and the purpose for which it is being processed. The controller is also responsible for making sure that outside contractors comply.
- Data Processor – They may be any groups that maintain and process personal data or any outsourcing firm that handles these activities. The data processor is held accountable for data breaches or non-compliance. Your company is also liable for penalties even if the fault lies entirely with the processing partner such as cloud provider.
- Data Protection Officer (DPO) - A designated DPO is must to oversee data security and GDPR compliance. Companies must have a DPO if they are a public authority, process or store a large amount of EU citizen data, process or store special personal data or regularly monitor data subjects. Some public entities such as law enforcement may be exempt from the DPO requirement.

Penalties and fines for Non-Compliance

General Data Protection Regulation (GDPR) allows steep penalties of up to €20 million or 4 percent of global annual turnover whichever is higher for non-compliance. GDPR sets a new standard for consumer rights about their data, but companies will be challenged as they put systems and processes in place to comply.

With the May deadline approaching fast, companies are hard pressed to follow GDPR regulations as compliance will cause some concern and new expectations from security teams.

For example, GDPR takes a wide view of what constitutes personal identification information. Companies will need the same level of protection for things like an individual's IP address or cookie data as they do for name, address and Social Security number.

This is a maximum fine that can be imposed for the most serious infringements, for example not having sufficient customer consent to process data or violating the core concept of Privacy by Design. There is a tiered approach to fines. A company can be fined 2% for not having their records in order, for not notifying the supervising authority and data subject about a breach, or for not conducting impact assessment. It is important to note that these rules apply to both the controllers and processors, meaning even the cloud providers will not be exempt from GDPR enforcement.

Business Impact for Industries

Any company that stores or processes personal information about the EU citizens within the EU states must follow the GDPR, even if they do not have a business presence within the EU.

Specific criteria for companies required to comply are:

- A presence in an EU country.
- No presence in the EU, but it processes personal data of European residents.
- More than 250 employees.

Fewer than 250 employees but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data. That effectively means almost all companies. A PwC survey showed that 92 percent of U.S. companies consider GDPR a top data protection priority.

According to the Article 3 of the GDPR, it specifies that if you collect personal data or behavioral information from someone in an EU country, your company is subject to the requirements of the GDPR. Two points of clarification should be noted:

- The law only applies if the data subjects, as the GDPR refers to consumers, are in the EU when the data is collected. EU laws apply in the EU. For EU citizens outside the EU when the data is collected, the GDPR would not apply.
- A financial transaction doesn't have to take place for the extended scope of the GDPR law to kick in. If the organization just collects "personal data", as part of a marketing survey, then the data would have to be protected GDPR-style.

Initial Preparation for GDPR

According to the EU GDPR official website, **Privacy by design** as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR.

The basic premise of this regulation is that data protection should be included from the onset of the designing of system's, rather than as an addition.More specifically, the controller should implement appropriate technical and organizational measures in an effective way in order to meet the requirements of this regulation and protect the rights of data subjects.

Article 23 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 only those needing to complete the processing.

- By pushing for a complete awareness of the organization's data web, GDPR forces business leaders to fully understand their data landscape (including their subsidiaries and partners)
- Complete documentation of all the data sources from all the origin countries
- Encourage data minimization (only required data is collected, planned use of the collected data, data deletion at the request of customers etc.)
- Develop and implement safeguards and security measures throughout your infrastructure to help contain any data breaches and taking quick action to notify individuals and authorities in the event a breach does occur (within the 72-hour time deadline).
- Consent of the customers must be freely given, specific, informed, and unambiguous. Pre-checked boxes and implied consent will not be acceptable anymore. Review all of the privacy statements and disclosures and adjust them where needed.

If you're interested to know more about how GDPR affects your customer data, then contact us today at https://www.gavstech.com/reaching-us/

About GAVS

GAVS Technologies (GAVS) is a global IT services & solutions provider enabling digital transformation through automation-led IT infrastructure solutions. Our offerings are powered by Smart Machines, DevOps & Predictive Analytics and aligned to improve user experience by 10X and reduce resource utilization by 40%.

For more information on how GAVS can help solve your business problems, write to inquiry@gavstech.com
www.gavstech.com

GAVS