



General Data Protection Regulation (GDPR)

by David Gumpfer

April 2018

How Europe's **New** Personal Data Rule **Impacts Real Estate**



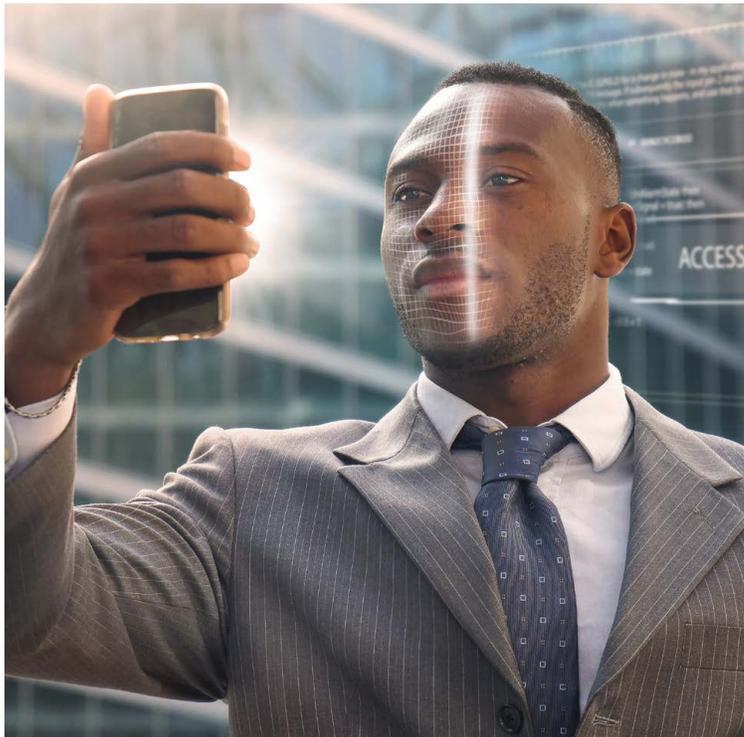
GDPR Takes Effect in Two Months. PREPARED?

////////////////////////////////////
General Data Protection Regulation (GDPR) compliance crisscrosses every business in the real estate industry. Yes, it's another acronym and it is not tech driven. *Well, almost not tech driven.*

“ What happens with our personal data afterward is entirely out of our control. We can only hope it is secure from access by hackers ... ”



Citizens from countries outside of the US are serious about protecting their personal privacy. Every time I’ve had data conversations with my European colleagues, they constantly stress how important it is to protect personal information.



While an important concern for us, most US citizens and companies are fairly indifferent on who we give access to our personal information.

What happens with our personal data afterward is entirely out of our control. We only hope it is secure from access by hackers – meaning those who steal data and misuse it for personal gain.

As we saw recently with Facebook and Cambridge Analytics – just like our EU colleagues – maybe US citizens should request to have more control over their personal data in the digital world.

GDPR as a Framework for Data Protection

The European Union (EU) enacted **GDPR** on April 27, 2016, as a framework to give back control of their citizens’ personal data across the globe.

GDPR was created because of the mandate out of the EU **Charter of Fundamental Rights** that citizens have a fundamental right to protect their own data.



When the GDPR was enacted, it replaced the 1995 EU Data Protection Directive as a national law. *The EU objective is to have one clear and concise data protection requirements across the board.*

If a company is found to be non-compliant with the GDPR, the fines are steep. The fines are from €10 million (\$12.3 million) or 2% of global revenue – whichever is higher – to €20 million (\$24.6 million) or 4% of global revenue.

GDPR commences on May 25, 2018. Two months from this week. It provides two primary objectives when developing the framework:

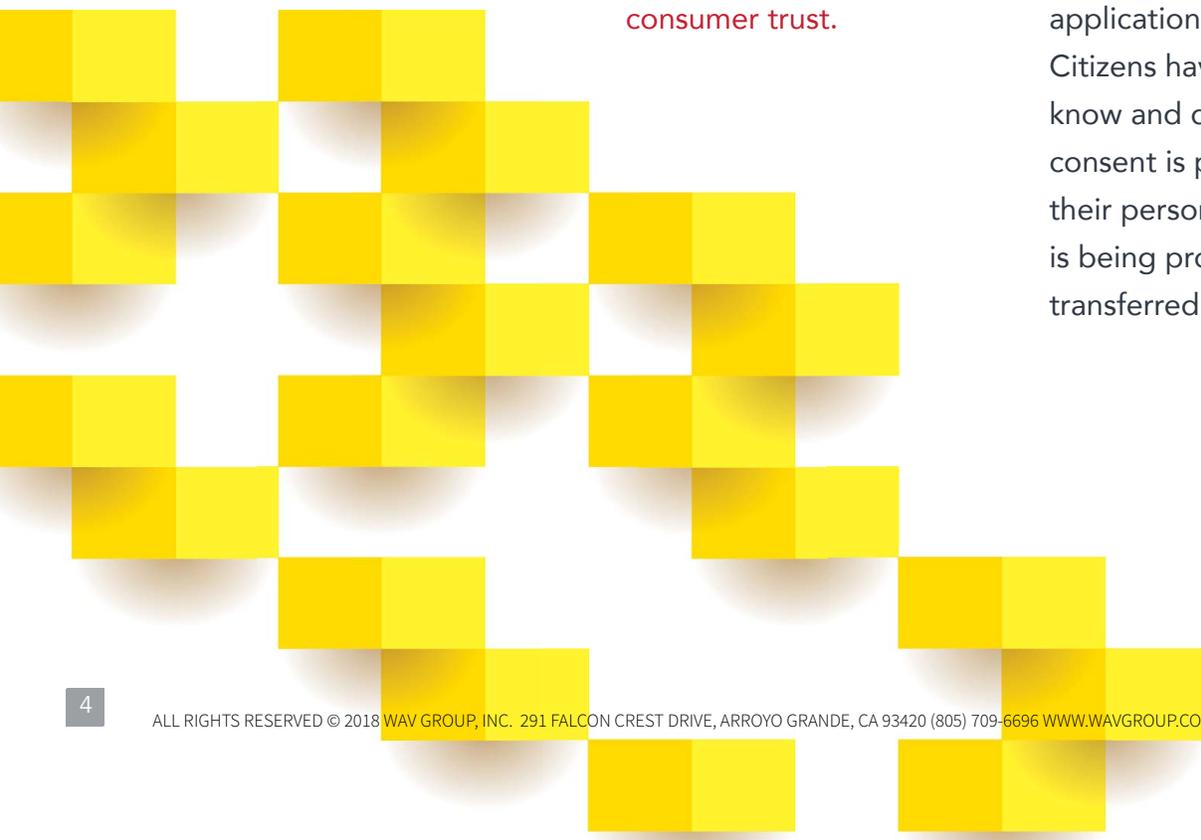
Provide more control and rights of EU citizens personal information back to the citizens – no matter where the data is stored or by whom – with modern and unified rules.

Define application and principles of data protection requirements to assist businesses in gaining consumer trust.



Rights of EU Citizens under GDPR

EU citizen rights to their personal information is enriched through the application of GDPR. Citizens have the right to know and decide – after consent is provided – how their personal information is being processed and transferred.





When an EU citizen makes a request through the **European Commission Data Protection Officer**, businesses must provide transparency of their usage and protection of a citizen's personal data.

EU citizens have the greater rights to erasure or "right to be forgotten." This supersedes the directive passed by the **European Parliament** in March 2014.

A directive created as a result of a judgment by the European Court favoring a **Spaniard's claim against Google**.

EU citizens have the right to willfully port their personal information from one provider to another without any interference by a National Data Protection Authority. A right to prevent one country from not allowing the citizen to have portability

of the personal information to a provider in a different country.

EU citizens have the rights to be immediately informed if unauthorized access has compromised their personal information.



For more detailed information and on the rights of EU citizens, visit the **European Commission's website**.



GDPR Definition of Terms

Before we get to how the GDPR impacts companies in the real estate industry, we need to understand the vernacular of some terms used in the GDPR .

I am going to warn you, the scope of these definitions are on the

fringe of throwing in the kitchen sink.

EU Natural Person:

An individual human being living in the EU. If your primary residence is in a member country of the EU, you have fundamental rights to protect your personal data.

Personal Data:

This is straight from the GDPR as it defines personal data 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, physiological,



genetic, mental, economic, cultural or social identity of that natural person”.

Processing:

The GDPR defines processing as, “...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

These two definitions pack a punch on how inclusive GDPR perceives what personal data is and the processing of the personal data.

Okay, now it’s time to get to the meat of the challenges GDPR presents to your real estate business.

GDPR IMPACT TO NON-EUROPEAN BUSINESS

The regulation is full of details, but let’s understand how GDPR is a concern for companies in the US.

US Company has a Presence or Subsidiary in One of the EU Member Countries

The company must comply with GDPR in protecting the personal data of any EU citizen. GDPR goes one step further under this article to include a provision that states compliance must be achieved no matter where the data is stored or processed throughout the enterprise.

A broad stroke of the brush to ensure companies doing business in the EU must provide the same fundamental rights of data protection across the globe. This removes any shield a company would use to

mitigate their need to comply to GDPR.

US Company Provides a Service or Product to EU Citizens

If the company provides a service or product to an EU citizen while the citizen is located within the EU territory, the company must comply to GDPR.

Under this article, real estate companies and public-facing MLSs with websites containing inquiry forms and user registration are potentially collecting an EU citizens personal data and must comply with GDPR.

Another area of concern is how real estate agents enter their customers' contact information into the MLS platform to receive 'Just Listed' notifications. The contact information could be from an EU citizen. Additionally, the industry has to tackle GDPR compliance

with listing agreements and sales contracts which are processed and sent for digital signatures to EU customers and stored on US systems.

Small and Medium Size Enterprises (SME's) Exemptions

GDPR criterion for compliance isn't based on the size of the company but on the company's activities in processing personal data. However, GDPR does provide some relief for micro, small, and medium-sized enterprises.

But!

There is a section in the GDPR that could easily mislead someone into believing that there are exemptions based on company size. GDPR exempts companies with less than 250 employees of having to record every activity of personal processing data. The catch – if the company

performs the process regularly – it must comply with GDPR and record every activity of processing the personal data.

Based on GDPR's definition of processing, sending emails or using systems to generate agreements and contracts to EU citizens – the company is required to comply, and the whole 250 employee exemption is thrown out the window.

I wondered if backing up the data falls under the criteria of regularly processing of personal data. My understanding is yes, data is processed during backup and stored in a different location. Remember GDPR is about the fundamental right for an EU citizen to control their own personal data and companies have to comply to protect that right.



Next Steps

Yes, this is a comprehensive initiative in protecting personal data and the impact to companies across the globe is significant. The following are high-level next steps which need to be owned and monitored by someone within an organization.

Awareness and Understanding of the Law

Start to research and understand what a company's obligations are in meeting compliance with GDPR. The **EUR-Lex website** is a great place to begin to understand the law.

Audit and Document Data

Now is the time to do a deep dive to validate if the personal data on your system contains citizens from the EU. This is going to be time-consuming but is

a best practice in a security protocol.

Develop a Roadmap

The roadmap guides the organization on remediation plans to fill the gaps in technology, policies, and procedures which create barriers of compliance with GDPR. This roadmap does include a section on Data Protection Impact Assessments (DPIA) and the tools required to help to document compliance and remediate citizens requests.

Assign a Data Protection Officer

If the company is required to comply with GDPR, assign a Data Protection Office. This role advises and informs others in the organization about their obligations to GDPR. Additionally, the role enforces and monitors ongoing compliance with GDPR.

Establish a Process

Define how the organization is going to react to citizen requests and procedures to accommodate the demands. Establish technology and policies ensuring data security is part of the organizations' routines and those policies are defined in the scope of new projects.

Train and Repeat

Implement training programs and repeat the process of security discovery and remediation to minimize the risks of non-compliance to GDPR. Every organization should have built-in functions to enforce and comply with their internal data protection protocols. Continuous training and policy evaluation reinforce a company's commitment to protecting their customers' personal data.



////////////////////////////////////
There is a lot more to know.

I only have touched the top of the GDPR iceberg. Does personal data include capturing a citizen's online behavior with cookies and device fingerprinting? Yes, it does!

There is also the agreement between the US, the EU, and with Switzerland called **Privacy Shield**. Privacy Shield is a framework offering these countries with compliance mechanisms to protect personal data. If a US company transfers personal data to another company, it probably should self-certify under Privacy Shield and create an addendum to their data sharing agreement to include compliance to GDPR.

At the very least, it is time to review your privacy policies and to research if there is personal data of EU citizens within the enterprise. If there

is, determine the exposure to the company and start the next steps.

At the End of the Day

GDPR will require companies to spend time and funds to reduce their risks of non-compliance. If you step back and look at the end result of being compliant, the benefits bolster an organizations ability to manage, maintain, and safeguard customers personal data.

Compliance to the law creates efficient data management, streamlined processes, transparency, better internal controls, data encryption, less long-term technology costs, and modernization of technology and processes.

As GDPR goes into practice on May 25, 2018, I am sure there are going to be

changes and challenges to the implementation of the law. There has been an understanding by the EU that not everyone is going to be compliant on this date. It is expected, however – that companies who qualify to comply – are on a pathway in providing greater data protection to consumers.

The WAV Group will continue to monitor GDPR and be a resource for the industry.

As there will be a need to modernize technology and policies, the WAV Group can continue to be a partner in providing assistance to implement new systems and process to be GDPR compliant.



About the Author

David Gumpper is a partner of the WAV Group as the Vice President of Technology Consulting.

David Gumpper has a foundation as a professional technologist in real estate, pharmaceutical, manufacturing and academia. David has spoken at events discussing technology and marketing in real estate at events by Leading Real Estate Companies of the World, Michael Saunders & Company, and Real Estate Standards Organization (RESO).

Gumpper's specialties:

Aligning technology with business strategy

Technology, security and vendor assessment

Application development leadership

CIO/CTO guidance

Product and project management

System Integration

Business process improvement

System conversion

About WAV Group

WAV Group provides consulting services that deliver equally on both strategic planning and technology and process implementation for enterprise brokerage organizations in real estate.

