

GENERAL DATA PROTECTION REGULATION

NEW EU DATA PRIVACY LAW MAY AFFECT US BUSINESSES

NAR LEGAL AFFAIRS
MAY 2018

On May 25, 2018, a sweeping new data privacy law goes into effect in the European Union (“EU”). The General Data Protection Regulation (GDPR) protects the personal data of EU residents and requires compliance by any entity that holds personal data of an EU resident. Additional guidance from the EU is forthcoming, and will likely provide clarity for entities, such as real estate brokerages and associations, with limited contacts with EU residents. There is also uncertainty regarding how EU regulators seeking to enforce the GDPR will obtain jurisdiction over U.S. entities. Additional guidance will be posted on nar.realtor when it is available.

GDPR’s Impact on Real Estate:

The GDPR does not impact entities that do not have, and do not plan to collect, the personal data of EU residents. However, U.S.-based real estate companies and REALTOR® associations that currently have, or plan to collect, the personal data of EU residents may be subject to GDPR compliance.

Real estate companies and REALTOR® associations may collect personal data of EU residents in a variety of ways. For example, an entity’s website may use online tracking tools, such as cookies, to collect data about an EU resident. An entity may maintain information about current and former clients and members that are EU residents. And, associations may have direct contact with current EU residents through a presence at trade shows, the sale of association products, or attendance at association educational sessions.

Personal Data Under to the GDPR:

The GDPR includes an extremely broad definition of the term “personal data”, and includes any information related to an EU resident, frequently referred to by the GDPR as the “data subject”, including any information that may lead to the identification of a data subject.

Consent is Required to Collect Personal Data:

The GDPR defines “consent” as a “freely given, specific, informed and unambiguous” indication that the individual provides, through an explicit statement or through a specific action, consent to the processing of the individual’s personal data. In order for consent to be valid, the identity of the “data controller”, the entity that determines what personal data is collected, and the intended purpose(s) for collecting the personal data must be made clear. In addition, the GDPR requires an EU resident to

provide affirmative consent prior to the collection of their personal data, which means that the required consent may not be obtained from a website's terms of use or other statements that presumes consent to the processing of their personal data. Keep in mind that an individual's consent may be withdrawn at any time.

The best way to obtain affirmative consent is to require a website user to affirmatively check a box consenting to the collection of their personal data. If the personal data is not collected via a website, then affirmative consent should be obtained at the point of collection, either electronically or in writing.

Rights of Data Subjects:

The GDPR provides every data subject with the following specific set of rights:

1. Right of Access: An individual may request confirmation from a data controller that it processes the individual's personal data and, if so, require that the data controller provide the individual with access to their personal data, as well a list of specific uses of the individual's personal data.
2. Right of Rectification: An individual may request corrections to inaccurate personal data or a supplement to incomplete personal data.
3. Right of Erasure (also referred to as the "Right to be forgotten"): An individual may request that the data controller erase all of their personal data.
4. Restriction of Processing: An individual may request that the data controller only process personal data upon the individual's consent.
5. Right to Object to Processing: An individual may object to specific uses of their personal data.
6. Right to Data Portability: An individual may request a copy of all personal data held by a data controller.

Vendors Collecting and Processing Data:

Companies may use third-party vendors to collect data or process data on their behalf. For example, a third party operator of a brokerage website may collect data for the brokerage. In this instance, the third party website operator is considered a "data processor", and the brokerage is considered the "data controller". Pursuant to the GDPR, the data controller is responsible for the actions of the data processor. Therefore, it is important that data controllers address GDPR compliance in its contract with data processors.

Preparing for the GDPR:

Entities subject to GDPR compliance should consider taking the following steps:

1. Conduct a Data Inventory.

Determine what personal data is in the entity's possession, and where the personal data is located. Personal data may reside in a number of places, including spreadsheets, databases, paper files, or with third parties acting on the entity's behalf. Once relevant data is identified, determine if there is a need to continue using the personal data and, if not, erase or remove the data from the entity's system.

2. Establish Process for Obtaining Consent.

Establish a process to obtain an individual's affirmative consent to the continued processing of their personal data, as well as from individuals whose data may be collected and processed in the future. For example, an entity could use a direct communication to affected individuals or obtain the required consent through the entity's website. Creating a pop-up box whenever an individual first visits the website that requires the individual to affirmatively consent to the collection and processing of their data is an effective way to obtain affirmative consent.

3. Establish Process for Responding to Requests.

Establish a process for how to receive and respond to a data subject exercising their rights articulated in the GDPR.

4. Contact Data Processors and Amend Contracts.

Address GDPR compliance by data processors acting on an entity's behalf. Include specific language related to GDPR compliance to new contracts, and be sure to amend existing contracts to ensure the data processor's GDPR compliance. Be sure to include a requirement that the vendor provide the entity with notice of any data breach, as well as an outline of the data processor's plans for complying with applicable law related to such breach.

Conclusion:

The vast majority of real estate companies and REALTOR® associations may determine that they are not subject to GDPR compliance because they do not collect or maintain personal data of EU residents. For those real estate companies and REALTOR® associations that have personal data of EU residents, and are subject to the GDPR, be sure to take steps necessary to comply.