CALIFORNIA ASSOCIATION OF REALTORS®

QUICK GUIDE

# Protecting Your Data – Tips for AORs and MLSs

Data looms large in our lives these days, and the real estate industry is no exception. Agent data, transactional data, and other types of data are becoming increasingly valuable assets that AORs and MLSs must protect. As entities that contract for a variety of products and services – for themselves as well as for members and subscribers – AORs and MLSs should be vigilant regarding how their data is being used and how to protect such data from unwanted usage. While some contracts directly focus on data, such as IDX agreements, even contracts that are not focused on data may touch on sensitive data. To protect data, AORs and MLSs should consider the following when entering into a contract:

- **Read the contract and vendor's privacy policy** – It is tempting to sign a contract without reading pages of legal text, especially if the contract is a click-through agreement or simply the Terms of Use (TOU) set forth on a vendor's website. However, carefully reviewing the contract will help you understand important terms, including whether any data is being used. You should also review the vendor's privacy policy (usually found on the bottom of the vendor's website) for additional information on how the vendor collects data, how the data is used, and whether you have any options on use of your data. If the contract is intended to supersede contradictory provisions of a TOU or privacy policy, makes sure it says so.
- **Specific terms to include** – If the vendor will have access to your data, make sure that the contract addresses the following:
    - **What data will be used and how** – Understand what kind of data (e.g., aggregated data, personally identifiable information, etc.) will be provided to the vendor and how the vendor is allowed to use the data. If you want to prohibit the vendor from using the data for certain purposes or in any way not provided in the contract, make sure the contract says so clearly. Most contracts will include a confidentiality clause that obligates the vendor to keep all data confidential, and only allows sharing in the intended ways.
    - **Data security** – What security measures does the vendor have in place to ensure that there will be no unauthorized access to the data? Keep in mind that the more sensitive the data (e.g., Social Security numbers or credit card information), the more stringent the security measures should be. Also, make sure that the vendor has a procedure in place to notify you of security breaches or other unauthorized access of the data. You may want a termination right in case of misuse by the vendor or unauthorized access of data.
    - **Data ownership** – The contract should be clear regarding who owns the data. In most cases, AORs and MLSs will likely want to retain ownership of all data provided to a vendor.
    - **Post-termination uses of data** – What will happen to the data you've provided once the contract terminates? Many contracts provide that the vendor will immediately stop using the data and return or destroy the data in its possession. If the vendor will retain the data, the contract should provide that the data remains protected as provided in the contract.
    - **Representations and warranties/Indemnification** – The vendor should represent and warrant that it will comply with all applicable security and privacy laws, and with PCI DSS standards for payment card data. As an added protection, you should require that the vendor indemnify you for third-party claims arising from the vendor's breach of applicable laws and policies, or its security, privacy, or confidentiality obligations under the agreement.
    - **Assignment/Change of Control** – the contract should provide that it can't be assigned without your consent, even by a change of control. If the vendor changes ownership or tries to assign the agreement anyway, the contract should allow you to terminate it, with liquidated damages if that makes sense.
- **Negotiate (if possible)** – Some agreements, such as click-through agreements, cannot be negotiated. However, whenever possible, try to negotiate to get the best possible protection for your data. Many vendors understand the concerns surrounding data sharing and are happy to work with their customers to reach mutually agreeable terms.