This is one of ten monthly alerts, counting down to the date when GDPR applies. **7** months to go

WOMBLE BOND DICKINSON

# Do Your Vendor Contracts Comply with GDPR?

Any entity processing personal data on your behalf (i.e., your vendors) must have a written contract in place. The GDPR requires specific language in your vendor contracts. **Review steps 1–4 below to bring your vendor contracts in compliance with the GDPR.**

**1** **Do we need to amend our existing vendor contracts?** If you answer "yes" to the questions below, then you will be required to update your vendor contracts (see step 4 below).

- Does the GDPR apply to our company?
- Does our company use third parties to process personal data on our behalf?
- Will the contract be in place on and from May 25, 2018 when the GDPR applies?

**2** **How do we amend our existing vendor contracts?** The amendment could take the form of a letter agreement or a more formal amendment. The amendment can take any form so long as it is in writing (including in electronic form), and it binds the processor to the controller.

**3** **What about any new vendor contracts?** You should also incorporate the requirements of Article 28 (see step 4 below) into any new contracts. You can include the required language in any form, such as in a schedule or in the main body of the contract.

**4** **What language must we add to our existing or new vendor contracts?**

You must describe the scope of the permitted processing, including the:

- ✓ Subject-matter and duration of the processing
- ✓ Nature and purpose of the processing
- ✓ Type of personal data to be processed and categories of data subjects
- ✓ Obligations and rights of the controller

Vendor must agree to:

- ✓ process the personal data only on documented instructions from you, unless otherwise required by applicable EU or Member State law
- ✓ ensure that persons authorized to process the personal data have committed to confidentiality obligations
- ✓ take all security measures required pursuant to Article 32
- ✓ not use a sub-processor without your prior written authorization
- ✓ assist you with responding to requests from data subjects
- ✓ assist you with your obligations relating to security, data breach notification requirements and data protection impact assessments
- ✓ return to you or delete, at your request, all personal data when services are completed, unless otherwise required by applicable EU or Member State law
- ✓ make information available to you to demonstrate vendor's compliance with the requirements of Article 28
- ✓ contribute to audits and inspections you or your auditors carry out

## Contact Us

If you have questions about this checklist or for additional information on the GDPR, contact Orla O'Hannaidh at orla.ohannaidh@wbd-us.com or +1 919.484.2339, or Amy Eames at amy.eames@wbd-uk.com or +44 (0)238 020 8379, or any member of our GDPR Compliance Task Force.

**Controller** is the entity which determines the purposes and means of the processing of personal data.

**Processor** is the entity which processes personal data on behalf of the controller.

**Processing** is any set of operations performed on personal data, such as collection, storage, use and disclosure.

**Personal Data** means information relating to an identified or identifiable natural person. A person can be identified from information such as name, ID number, location data, online identifier or other factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.