Federal Contractors Must Provide Privacy Training: Follow The 5-Step Plan To Ensure Compliance

Insights
1.23.17

Effective immediately, federal contractors will need to comply with privacy training rules intended to ensure that their workforces protect personally identifiable information. As of January 19, 2017, federal contractors will need to follow a five-step plan to comply with the new rules issued by the Department of Defense, General Services Administration, and National Aeronautics and Space Administration.

Step One: Identify
The first step in the process requires you to **identify** those individuals who are now subject to the privacy training rules. These include workers who:

- Have access to a system of records;
- Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle "personally identifiable information" on behalf of the agency; or
- Design, develop, maintain, or operate a system of records.

The rules also define personally identifiable information (PII) as any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Step Two: Train
Once identified, the second step requires you to **train** them on their privacy obligations. The rules require you to get them up to speed on all of the key elements necessary for ensuring the safeguarding of PII or a system of records. The training must be role-based, and must provide both foundational and more advanced levels of training. It also must be measurable, including a system to test the knowledge level of those receiving the training. After the initial training, it must be provided annually thereafter.

The rules include the following minimum topics to be included for the training:

1. The provisions of the Privacy Act of 1974, including penalties for violations of the Act;
2. The appropriate handling and safeguarding of PII;

3. The authorized and official use of a system of records or any other personally identifiable information;
4. The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access PII;
5. The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of PII; and
6. Procedures to be followed in the event of a suspected or confirmed breach of a system of records or unauthorized disclosure, access, handling, or use of PII.

Those required to offer the training can do it themselves or can use the training from another agency (unless the contracting agency specifies that only its training is acceptable for its purposes).

Step Three: Maintain Records
The rules require you to also **maintain** documentation to prove that all applicable employees received the mandatory training. Upon request, you must provide this information to the federal agency.

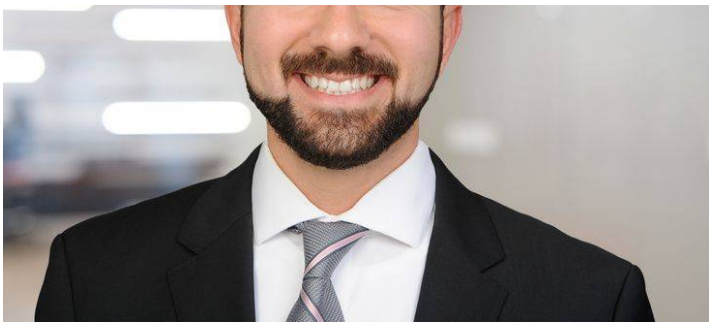
Step Four: Flow-Down
If you are a prime contractor using the services of subcontractors, the rules also require you to **flow-down** these requirements to all applicable subcontractors.

Step Five: Prohibit
Finally, you must **prohibit** any and all contractor employees who have not completed the privacy training from performing certain tasks. You are required to ensure they do not have or retain access to a system of records; create, collect, use, process, store, maintain, disseminate, disclose, or dispose, or otherwise handle PII, or design, develop, maintain, or operate a system of records.

If you have any questions about these rules or how it may affect your business, please contact any member of our Affirmative Action and Federal Contract Compliance Practice Group, our Data Security and Workplace Privacy Practice Group, or your regular Fisher Phillips attorney.

This Legal Alert provides an overview of a finalized new federal regulation. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Richard R. Meneghello
Chief Content Officer
503.205.8044
Email

Susan M. Schaecher
Senior Counsel
303.218.3650
Email