

Table of Contents

I	Background
II	When the GDPR Applies
III	How the GDPR Impacts Commonwealth Agencies
IV	What about vendors/suppliers sending GDPR notices?
V	References

I. Background.

On May 25, 2018, the European Union’s (EU) Regulation 2016/679 – “General Data Protection Regulation” (GDPR) went into effect. The GDPR replaces the 20- year old EU Directive 96/46/EC. The GDPR recognizes the protection of people in relation to processing of their personal data as a fundamental right. The GDPR aims to ensure a consistent and high level of data protection across all EU member states.

The GDPR regulates the electronic collection, storage, processing, and disclosure of “personal data” relating to individuals residing in the EU. The GDPR defines “personal data” as “any information that relates to an identified or identifiable natural person (‘data subject’)” and includes data that has been de-identified, encrypted, or anonymized but that can be used to re-identify a person. The following are examples of “personal data”:

- a name;
- an address, whether physical or email;
- an identification number;
- location data;
- an online identifier.

The provisions of the GDPR will become clearer over time, as the EU interprets, applies, and enforces it.

II. When the GDPR Applies.

The GDPR frequently uses the term “processing,” which it defines broadly to include the “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction” of personal data. The GDPR applies whether processing is by automated or non-automated means.

Many companies have revised their privacy policies, practices, and technologies, or have sought new consent related to personal data, even outside the European Union, because the GDPR applies to:

- an entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; and

- an entity established outside the EU that offers goods/services (paid or for free) to individuals in the EU or monitors the behavior of individuals in the EU.

A company or organization may find a need for GDPR compliance if it: (1) is established in the EU; or (2) offers goods and services to, or monitors the behavior of, individuals within the EU.

III. How the GDPR Impacts Commonwealth Agencies.

In many cases, the GDPR is unlikely to impact Commonwealth of Virginia (CoVA) public bodies directly because many Virginia public bodies do not operate within the EU or interact with individuals in the EU. If a public body does so, however, it should work with its legal counsel regarding its European activities and interactions with individuals in the EU.

The GDPR may impact Virginia public bodies indirectly in two ways. First, Virginia public bodies may be customers of global companies that revise their own policies, practices, and technologies in light of the GDPR. Second, Virginia public bodies may see requests from vendors or suppliers related to the GDPR, as discussed in the next section.

IV. What about vendors/suppliers sending GDPR notices?

Because of the broad scope of the GDPR, many vendors and suppliers that provide goods and services to CoVA are subject to the GDPR. To address this, many of these vendors/suppliers are revising their contracts so as to facilitate their own compliance with the GDPR. It is important to keep in mind that standard state contract terms (i) make CoVA "personal data" that a vendor/supplier may have subject to VITA's security standards and so may already bar storage and processing outside of the United States, and (ii) apply data security laws of the United States of America and the Commonwealth of Virginia. If a Virginia public body receives a request from a vendor/supplier for contract change related to the GDPR, the public body should contact and work with their legal counsel to assess the need for and acceptability of the proposed change.

V. References.

[Regulation \(EU\) 2016/679](#) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).