The European Data Protection Board recently requested comments on its data protection “by design and default” guidelines. Comments are due by mid-January of next year. The Guidelines provide clarity about how to address GDPR’s requirement that companies take “appropriate” technical and organizational steps to protect personal information and individuals. Part of the law’s requirements, according to the guidelines, is that companies can show that the measures they took are effective.

The guidelines stress that measures taken must be appropriate and integrate “necessary safeguards” into the processing of personal information. Measures might range from training to use of advanced technical tools. Examples of potentially appropriate safeguards might include, according to the Guidelines, data deletion reminders, malware detection systems, pseudonymization of data, or training employees about phishing. Important to the EDPB is that companies can demonstrate that the measures they took are designed to protect “data subjects rights and freedoms” as those are set out in GDPR (Articles 12-22). The Guidelines suggest that companies can use key performance indicators to measure compliance, such as looking at quantitative measures (fewer complaints, faster response time) or qualitative ones (expert assessments, grading scales). The company could,
alternatively, show their rationale for how they have chosen to assess the effectiveness of the safeguards they selected.

With respect to the concept under GDPR of using “state of the art” measures, the EDPB clarifies in the Guidelines that this means thinking about currently available technologies and organizational measures, and thus staying up-to-date on what is available in the market. The Guidelines state that this requirement under GDPR is dynamic, and thus a company that was at one point compliant may no longer be so in the future if it fails to keep up with developments. The Guidelines also provide input on extent of processing, storage limits, and accessibility, among other details.

The Guidelines conclude by providing examples of operationalizing the data by design approach (which the EDPB calls DPbDD). One, for example, is of a company that is considering purchasing a CRM platform to let it centralize the information it maintains about its customers. The CRM will also let the company pull in public information and better assess its customers “purchasing power.” To address the requirements of DPbDD, the EDPB example has the company require of the CRM platform provider that it map the processing activities within the CRM to the purposes relevant to the company, and flag when processing activities are not aligned with the company’s legitimate purposes. The company can then consider to either (1) establish a new legal basis for processing or alternatively (2) not use that part of the CRM platform tool.

After the public comment period closes on 16 January 2020, the Guidelines will be finalized by the EDPB.

Putting it Into Practice: Companies operating in Europe should review these guidelines carefully, as they provide detailed information about expectations from the EDPB regarding security by design. Of particular interest are the examples provided by the EDPB for different ways to operationalize DPbDD.

Copyright © 2020, Sheppard Mullin Richter & Hampton LLP.