Viewing the GDPR Through a De-Identification Lens:
A Tool for Clarification, Compliance, and Consistency

Mike Hintze[1]

Abstract

In May 2018, the General Data Protection Regulation (GDPR) will become enforceable as the basis for data protection law in the European Economic Area (EEA). The GDPR builds upon many existing concepts in European data protection law and creates new rights for data subjects. The result is new and heightened compliance obligations for organizations handling data. In many cases, however, how those obligations will be interpreted and applied remains unclear.

De-identification techniques provide a range of useful tools to help protect individual privacy. While there is disagreement on certain aspects of de-identification and the degree to which it should be relied upon, there is no doubt that de-identification techniques, properly applied, can reduce privacy risks and help protect data subjects' rights. In order to further these key objectives, regulatory guidance and enforcement activity under the GDPR should encourage and reward the appropriate use of de-identification.

Fully recognizing the role that de-identification can and should play can also help bring clarity to many GDPR requirements and can provide a helpful tool for compliance. Moreover, it can help create a bridge between European data protection rules and the different approaches to privacy regulation in the United States and elsewhere. But achieving these goals requires an explicit recognition that there is a wide spectrum of de-identification, and that different levels of de-identification have different regulatory and policy implications.

This article will examine a number of obligations under the GDPR, including notice, consent, data subject rights to access or delete personal data, data retention limitations, and data security. In each case, it will describe how the use of different levels of de-identification can affect the application and interpretation of the requirements and resulting compliance obligations, as illustrated in the following chart (which will be explained more fully in article).

<table>
<tr><th>Level of Identifiability</th><th>Notice to Data Subjects</th><th>Consent or Legitimate Interest</th><th>Data Retention Limitations</th><th>Appropriate Data Security</th><th>Access, Deletion, Controls</th><th>Online Advertising Choice</th></tr>
<tr><td>Linked</td><td rowspan="3">Prominent Notice
⇕
Discoverable Notice</td><td rowspan="3">Consent of Data Subject
⇕
Legitimate Interest</td><td rowspan="3">Shorter Retention
⇕
Longer Retention</td><td rowspan="3">Stronger Protections
⇕
Some Protections</td><td rowspan="2">Required</td><td>Opt-In</td></tr>
<tr><td>Linkable</td><td>Opt-Out</td></tr>
<tr><td>De-Linked</td><td rowspan="2">No Requirement</td><td rowspan="2">N/A</td></tr>
<tr><td>Anonymous / Aggregated</td><td colspan="5">No Requirements</td></tr>
</table>

The article will argue that the GDPR requirements in each area can and should be interpreted in a way that will encourage the highest practical level use of de-identification and that doing so will advance the purposes of the regulation.

[1] Chief Privacy Counsel, Microsoft Corporation