GDPR compliance steps, and impacts on MDM thinking

The impacts of the General Data Privacy Regulations are tremendous and cannot be overstated for any business that deals in personal or private data. In large enterprises, the subject of Master Data Management is often a 3rd rail, or considered a sure path to career death due to the complexity of the topic. Done properly the benefits are tremendous, but the ownership of information at the functional level is so often a barrier to success that it has become generally understood that these efforts are rarely fully successful.

Now we enter the world of GDPR. The regulation in principle is simple. It can be generalised to say: If you collect any personal information (broadly defined) you must make the information owner aware of what you collect, what you do with it and how to get that information back or purge it.

While it sounds simple in application, the complexity of the average enterprise information ecosystem makes this horrendously challenging. In the pharmaceutical industry where I currently work, patient information is collected in the course of a number of activities. As a part of that, various systems and reports are impacted and the process gets exponentially more complicated when biospecimens (samples of tissue, blood, etc…) are concerned. All samples must have consent for use documented, and a traceability through the full lifecycle. When data is “blinded” or anonymized, this adds even more complexity as the ramifications of “unblinding” data are significant to the integrity of the overall trial process. Beyond patient data, there is data on clinicians, research organizations, collaborators and more.

My recommendations I have made, and I suggest to clients include the following:

1. A comprehensive audit of all Personally Identifiable Information collected or generated in the course of business. This should result in a list of data attributes, source of collection, systems and processes impacted
2. For all data collected, where mastering or simplification of process is feasible, a plan must be defined and should be mapped into an overall value stream analysis for inclusion in a portfolio of work focused on GDPR compliance.
3. All data once mapped, must be included in a reference that allows comprehensive aggregation of the record – unifying the person to a single view. This requirement is where the value of mastering comes to the top. Without the ability to view a person in a record, the next step is exponentially more challenging.
4. The Data Privacy Officer for the company and if applicable, related functions, must be pulled in to evaluate the plans and approach, supplementing the data record or approach as needed.
5. The next step in compliance once the data is clearly mapped and understood is an evaluation of the impact of “providing and purging” as each data owner has the right to request at any time a comprehensive export of all data collected about them. Correspondingly, they can also request that all personal data be purged. This becomes particularly challenging when data has cross dependencies and is a part of a larger analysis.
6. The evaluation of the provide and purge process must result in a documented program and process to answer the question of what is the impact of a request. How will we mitigate the risk and what needs to change about our processes to accommodate these needs. This starts with the evaluation, moves to a

documented plan, and then must be accompanied by at a minimum, a tabletop exercise of the multiple scenarios identified.

This is a costly effort, from a time and resources perspective. As an enterprise, leaders must be aware of the risk of non compliance relative to the cost of compliance.