Drafting Robust TOMs - a Blog Post by Michael Whitener

“TOMs,” for those unversed in GDPR acronyms, refers to the “technical and organizational measures” for keeping personal data secure required under the GDPR (Art. 32) as well as under the standard contractual clauses (Annex II).

Compared with the EU Data Protection Directive it replaced, the GDPR takes a more granular approach to security requirements. While both the Directive and the GDPR require TOMs “appropriate to the risk,” the GDPR adds a list of measures to include “as appropriate,” including pseudonymization and encryption of personal data, the ability to restore personal data if there is an “incident,” and a process for regularly testing, assessing and evaluating the TOMs.

TOMs must be included in a data processing agreement (DPA) under GDPR Art. 28(3)(c), which requires that a processor “takes all measures required pursuant to Article 32.” As I noted in an earlier blog post, TOMs tend to be one of the “pain points” in negotiating DPAs.

Occasionally a processor will try to skate by in its DPA with just quoting the GDPR requirements. Essentially that processor is saying to the controller: “Yes, we’ve implemented appropriate TOMs. Trust us.” But that approach just encourages the controller to attempt to impose its own (often quite onerous) security requirements on the processor.

A better approach is for the processor to lead with its own robust TOMs. A proposed structure for TOMs that includes all the elements required under GDPR Art. 32 is as follows:

Data Confidentiality

Physical Access Controls (e.g., alarm system, video surveillance, visitors’ protocol).

Logical Access Controls (e.g., technical measures such as firewalls and encryption; organizational measures such as user permission management).

Authorization Controls (limiting access to authorized users).

Separation Controls (separating the processing of data collected for different purposes).

Pseudonymization (preventing attribution of personal data to an individual without the use of additional information that is maintained separately).

Data Integrity

Transfer Controls (protecting data during electronic transmission or while transported/stored on data media).

Input Controls (limiting the entering, modifying and deleting of data; e.g., by technical logging measures).

Data Availability and Resilience

Availability Controls (protecting data against accidental destruction or loss; e.g., use of separately stored backup media).

Recoverability Controls (ensuring the ability to rapidly restore data availability and access in the event of a physical or technical incident).

Testing, Assessment and Evaluation

Data Protection Management (e.g., appointing a Data Protection Officer; annual review of the effectiveness of the TOMs and revising as appropriate).

Incident Response Management (documented process for detecting, handling and reporting security incidents/data breaches).

Data Protection by Design and by Default (consistent with GDPR Art. 25, ensuring that data protection principles are "built in" to the development and design of products, services and applications and that personal data collection is minimized).

Subcontractor Management (conducting security reviews of subcontractors handling personal data; entering into data processing agreements; and monitoring subcontractor performance).

If the processor has obtained certifications such as ISO 27001 or undergoes annual SOC 2 Type 2 audits, that should be highlighted as well, since these certifications/audits indicate the processor's security protocols have been vetted by a qualified third party. (Note that GDPR Arts. 42 and 43 specifically address certification and certification bodies, respectively.)

One concern I sometimes hear voiced about committing to detailed TOMs is that the processor gets locked into the TOMs as described, thus robbing the company of flexibility to adapt the TOMs to changing technology and business conditions. For instance, what if your TOMs state that you use AES-256 for encrypting data at rest, and an even more robust encryption method comes along that you decide to adopt. Are you at risk of breaching the TOMs referencing AES-256 encryption you've previously agreed to?

That concern can easily be addressed by building in flexibility to the TOMs themselves. A couple of real-life examples serving this purpose:

"*The technical and organizational measures are continuously improved by [Company] according to feasibility and state of the art and brought to a higher level of security and protection.*"

"[Company] may change these security measures at any time without notice so long as [Company] maintains a comparable or better level of security. Individual measures may be replaced by new

measures that serve the same purpose without diminishing the security level protecting personal data.
”

The GDPR drafters were pragmatic enough to recognize that no one size fits all when it comes to security measures, and a utopian world of perfect security doesn’t exist. As long as your TOMs are aligned with (1) the nature of the personal data you collect, (2) the risks that the loss or misuse of such data would pose to data subjects, and (3) the technological state of the art with respect to protecting such data, you’re in good shape.