PERSONAL DATA PROTECTION COMMISSION SINGAPORE

PRACTICAL GUIDANCE TO ZUELLIG PHARMA

Background

1. Zuellig Pharma (ZP) implements a Privacy Enhancing Technology (PET) solution in ZP's environment, and allows authorised users, including third party organisations (TPOs), to access and use the solution. Essentially, a TPO that wants to make use of the PET solution will transfer the relevant data into a secure region of ZP's environment ("Trusted Execution Environment" or "TEE"). Technical safeguards prevent ZP and other third parties from reading, modifying, or otherwise accessing the data transferred by that TPO into the TEE.

2. Next, the TPO will use a web application provided by ZP to apply the SHA-256 hashing algorithm to fields of the transferred data that contain personal or sensitive data. The same web application can be used by the TPO to transfer the hashed data out of the TEE, and to permanently delete the data that the TPO transferred into the TEE. The TPO can also program the TEE to permanently delete the transferred data after a specified period of time.

3. ZP sought guidance from the Personal Data Protection Commission (PDPC) on whether the TPO's transfer of personal data into ZP's TEE constitutes disclosure under the Personal Data Protection Act 2012 (PDPA) such that the TPO is required to obtain consent from the individuals to whom the personal data relate.

PDPC's assessment

4. Based on the information above, PDPC is of the view that the TPO is engaging ZP as a data intermediary (DI) to provide hashing services through ZP's TEE and web application[1]. PDPC has given guidance that express consent is not necessary for an organisation to share personal data with its DI to process personal data on its behalf, provided that the personal data is not used by the DI for other purposes without the consent of the individual[2]. In this case, since ZP will not use or even access the personal data for other purposes, the TPO may transfer personal data into ZP's TEE without obtaining consent from the individuals.

5. Having said the above, PDPC has three further comments. First, the contract between the TPO and ZP should make clear what scope of work ZP is to perform on the TPO's behalf and for its purposes, e.g. providing the TEE and the web application for hashing, and each party's responsibilities and liabilities in relation to the transferred personal data.

[1] An analogy is an organisation engaging a cloud service provider as a data intermediary to provide cloud services.
[2] See PDPC's **Guide to Data Sharing**, at para 1.8.

6. Second, as a DI of the TPO, ZP is subject to the Protection, Retention Limitation, and Data Breach Notification Obligations. PDPC notes that ZP has put in place technical safeguards to protect the transferred data, and that the web application ensures the deletion of the transferred data (either when the hashed data is transferred out or upon the expiry of a period of time specified by the TPO). These measures help ZP meets its Protection and Retention Limitation Obligations in the TEE implementation. Under the Data Breach Notification Obligation, where a data breach[3] is discovered by ZP, ZP is required to notify the TPO without undue delay from the time it has credible grounds to believe that the data breach has occurred.

7. Finally, while hashes are cryptographically generated strings that serve as irreversible one-to-one representations of the data that was hashed, proper safeguards should be implemented to prevent attackers from identifying individuals through inferences from pre-computed tables. ZP and the TPO may wish to ensure that the hashes generated should be reasonably strong (e.g., by using industry-standard algorithms and incorporating a salt) to protect the data, particularly in the case of data that follows pre-determined formats or parameters such as NRIC numbers and race. ZP and the TPO can refer to PDPC's Guide to Basic Anonymisation and Guide on Data Protection Considerations for Blockchain Design on safeguards that organisations should consider when using hashing techniques to protect personal data.

END OF DOCUMENT

[3] "data breach", in relation to personal data, means —
(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or
(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.