Wednesday, June 27, 2018 1:36:13 PM

Ruud Leurs

Rationale	**Information Security for Surveys**
Description	Surveys process in almost all cases, confidential information (personal data). These should therefore be set up carefully.
Supplement	How to handle the information security aspects that are relevant to the implementation and execution of surveys? Context for surveys these days is an electronic way of presenting them (portals), but the essence of the requirements is not limited to this. 1. The information within a survey must be classified as confidential. 2. Because of the classification of the information, it must have a designated owner (in person). 3. Before any communication about the survey occurs, the survey must be reviewed with a KPN Privacy Officer and the interviewer / pollster needs to obtain his/her approval. 4. The (electronic) communication about the survey must originate from within a KPN domain. The authenticity and correctness of messages must be verifiable by recipients. This holds for all forms of communication. If messages are reply-able, the replies must go to the originating KPN domain. Articles, explanations etc. should be posted on the KPN intranet; e-mail communication only from (and reply-able to) an @kpn.com mail address. Link targets in for example (but not limited to) e-mail messages or TeamKPN postings must be hosted within- or routed/redirected via the KPN domain. A direct link to an outside resource is not allowed. In general sense, e-mail communication about a survey must comply with the relevant requirements from the policy **'Securing e-mail'** (KSP-RA-359). 5. A call for participation cannot just “pop up” all of a sudden – the population must be informed about the survey at an earlier moment in time. This eliminates extra traffic to the helpdesk “is this a phishing mail” and similar questions. 6. The web portal that presents the survey must be protected against unauthorized access. There are multiple ways of achieving this: • Username + password + brute force lock out at the portal; • Single sign on via grip (but be careful with surveys that claim anonymity); • A “random” string of characters in for example the URL within the personal invitation to participate. The string must be long, not enumerable and the portal must have a brute force lock out facility. A URL example: https://queeste.kpn.com/MO-2Q17/ 6be4c40b2d4db3b714bf9e932aeee196a4586c33fe57242ced9c01b5e251fd3f

	in which the part in red type is obtained by feeding a user-ID and a salt through an acceptable hash function (sha256 in this case). The resulting long URL must be distributed as-is (and not be fed through a URL-shortener). 7. With all involved external parties, a data processor agreement must be signed. In this agreement, a detailed limitative description of the transferred data objects as well as the purpose of data processing must be included. If, with a particular 3rd party, an existing data processor agreement is already in place it must be reviewed and possibly modified to obtain compliance with this document. Depending on the contract value with a 3rd party, the establishment of a Data processor agreement is taken care of via Corporate Procurement Office, or one can compile the basis of an agreement document by using the materials found in the Legal & Regulatory DIY portal. In both cases the final result before signing requires the approval of a KPN Compliance Officer. 8. If desired the survey results must, after processing, be archived according to Storing confidential information. When the survey implementation and/or execution involves a 3rd party that processes KPN data, it must be established and agreed upon that this party will destroy all PII and other (including raw) data after aggregation and reporting. 9. In the case KPN will develop and implement a web portal and will host this as well. This must be regarded as an Innovation and Development activity and should be treated according to Security measures in innovation and development. 10. In the case KPN contracts an external party to build and/or implement the survey. The resulting web portal (for example) can be hosted within or outside the KPN domain. With each external party a Security Annex need to be established and agreed upon.
Subject Area	Information handling and asset management
ID	KSP-RA-686
Version	1.1
Date	June 18, 2018