CERTIFICATION REQUIREMENTS OF MANAGEMENT SYSTEM

ANNEX C
ISO/IEC 27701:2019

ADDITIONAL INFORMATION/REQUIREMENTS FOR THE AUDIT

1. Certification according to ISO/IEC 27701 requires that the Organization:
   a) Is applying simultaneously for ISO/IEC 27001 certification, or
   b) Is already certified* for ISO/IEC 27001, and its certificate is active.

   Note b): Certified for ISO/IEC 27001 by Q-CERT or another accredited certification body.

   In case you apply for a certification audit for ISO/IEC 27701 only, you should be aware that additional time will be required to audit the main management elements of the ISO/IEC 27001 system you are implementing.
2. The validity period of the certificate is inextricably linked with that of ISO/IEC 27001.
3. Accordingly, if for any reason the validity of the ISO/IEC 27001 certificate is not renewed, suspended or terminated, the validity of its ISO/IEC 27701 certificate is automatically suspended or terminated.
4. The scope of the Organization's management system for ISO/IEC 27701 may be different from that of ISO/IEC 27001,

   i.e., it may cover specific services/products/processes provided that the above are included in the scope of ISO/IEC 27001.
5. The Organization may have one common "Statement of Applicability" covering both standards or two separate ones.
6. The duration of the audit in both cases (combined for both standards or separate for ISO/IEC 27701) is determined by the supporting standards and by the requirements of the Accreditation Body. It also depends on the role of the Organisation in terms of the management of Private/Personal Information (PII) i.e., whether it simply processes the information or whether it is the controller of the information or whether it both controls and processes the information.
7. If during the inspection it is detected that the role declared by the Organization through its application does not correspond to the reality, then the inspection time and the cost of the inspection will be modified (in consultation with Q-CERT headquarters).
8. In case that the audit is not combined for both standards, the auditor(s) will also carry out an audit of key elements of the Information Security Management System (ISO/IEC 27001) such as, for example, internal audits and management review.

Note: This, together with the certification regulation, form part of the commitments that the customer signs that he accepts through the contract (F-2002) with the Certification Body.

ANNEX C
ISO/IEC 27701:2019

ADDITIONAL INFORMATION/REQUIREMENTS FOR THE INSPECTION

The role of the Organization (client) in relation to the Management of Private/Personal Data

The Organization (client) should define and responsibly declare to us its "role" in relation to the Management of Private/Personal Information, i.e., whether:

- ✓ Just process such information (processor), or
- ✓ Is the controller of such information, or
- ✓ It controls and processes such information (processor & controller).

The following information/explanations are given to help you choose the right one:

1. ***"Processor":***

   Processes private/personal data only on behalf of the "controller". Therefore, the data controller does not "own" or control the data it processes. This means that it cannot change the purpose and means by which the data is used. Following the example above, the data processor is the third-party company that the data controller chose to process the data.

   Data processors are bound by the instructions given by the data controller.

2. ***"Controller":***

   The controller shall determine the purposes for which and how the private/personal data are processed. Controllers take decisions on processing activities, exercise overall control over the private/personal data processed and are ultimately responsible for them and for their processing.

3. ***"Processor & controller":***

   When its activities cover both above situations.

Example:

A polling company (A) that carries out the whole data collection process has contracted an IT company (B) to analyze the data and send it to the stakeholders. (A) determines the data to be used, the format that the results of the analysis should be in and the how to capture/present them in a report in a defined format, (B) analyses the data, stores it in its system, prepares the report and sends it to the client as specified by (A). In this case, company (A) is the "Controller" and (B) is the "Processor".

Attention:

Providers of specialized services, e.g., accountants, are always considered as controllers. The reason for this is because they must work to certain professional standards and are required to take responsibility for any personal data they are hired to process. For example, if the accountant discovers an unfair practice when completing the company's accounts, he or she may be expected to report this malpractice to the police or other authorities. If they are forced to take this action, they will no longer be acting on their client's instructions, but in accordance with their own professional obligations and therefore as data controllers. Specialist service providers who process data in accordance with their own professional obligations will always act as controllers.

Note: This, together with the certification regulation, form part of the commitments that the customer signs that he accepts through the contract (F-2002) with the Certification Body.