This applies only to Organizations / Companies which apply for certification to ISO/IEC 27001 and/or ISO/IEC 27701 Standard.

**Questo vale solo per Organizzazioni / Aziende che richiedono la certificazione secondo lo standard ISO/IEC 27001 e/o ISO/IEC 27701.**

Please fill-in the following information. **For sections 1 to 7 check the description (a, b or c) which best describes your organization. In case of multiple sites, which have significant differences between them, please fill in a separate Annex D form for each different site.**

Si prega di compilare le seguenti informazioni. **Per le sezioni da 1 a 7 barrare l’opzione (a, oppure b, oppure c) che meglio descrive la propria organizzazione. In caso di più siti, con differenze significative tra di loro, si prega di compilare un ANNEX D per ogni sito**.

**NOTE: Keep in mind that for ISO/IEC 27701 you must have a valid / active ISO/IEC 27001 certificate and if not, you have to apply for both standards.**

**NOTA: Si tenga presente che per ISO/IEC 27701 si deve avere un certificato ISO/IEC 27001 valido/attivo e, in caso contrario, si devono richiedere entrambi gli standard.**

**The application is for/ La richiesta è per::**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ISO/IEC 27001 | ... | Combined / Entrambe ISO/IEC 27001 & ISO/IEC 27701 | ... | ISO/IEC 277011),2) | ... |

**1)In this case / In questo caso**

|  |  |  |  |
| --- | --- | --- | --- |
| You have an active / valid ISO/IEC 27001 certificate issued by Q-CERT  Si è in possesso di un certificato ISO/IEC 27001 attivo/valido rilasciato da Q-CERT | ... | You have an active / valid ISO/IEC 27001 certificate issued by another accredited CB **(pls send us)**  Si è un possesso di un certificato ISO/IEC 27001 attivo/valido rilasciato da un altro OdC accreditato **(si prega di fornirlo)** | ... |

**For/Per ISO/IEC 27701:**

**a) You act as a / Vi comportate come un:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Processor / Processore | ... | Controller / Controllore | ... | Processor & Controller / Processore & Controllore | ... |

***"Processore":***Tratta i dati privati/personali solo per conto del "responsabile del trattamento". Pertanto, il responsabile del trattamento non "possiede" o controlla i dati che tratta . Ciò significa che non può modificare le finalità e i mezzi con cui i dati vengono utilizzati.

***"Controllore":*** Il responsabile del trattamento determina le finalità e le modalità di trattamento dei dati privati/personali. I responsabili del trattamento prendono le decisioni sulle attività di trattamento, esercitano un controllo generale sui dati privati/personali trattati e sono responsabili in ultima istanza degli stessi e del loro trattamento.

**b) Activity scope if different from ISO/IEC 27001 (must be within the boundaries of ISO/IEC 27001 scope) / Ambito dell'attività se diverso da quello della ISO/IEC 27001 (deve rientrare nei limiti dell'ambito della ISO/IEC 27001)**

|  |
| --- |
| Describe / Descrivere: |

**c) Number of sites if less from those stated for ISO/IEC 27001 (location(s) / address(es) / building(s)) / Numero di siti se inferiore a quelli indicati per la ISO/IEC 27001 (ubicazione/i / indirizzo/i / etc/ecc):**

|  |
| --- |
| Describe / Descrivere: |

**d) The extent to which the main activity of the Organization requires PII processing / La misura in cui l'attività principale dell'Organizzazione richiede l'elaborazione delle PII:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rarely / Raramente | ... | Occasionally /Occasionalmente | ... | Systematically / Sistematicamente | ... |

**e) The extent to which the main activity of the Organization entails the processing of sensitive PII / La misura in cui l'attività principale dell'Organizzazione comporta il trattamento di PII sensibili:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rarely / Raramente | ... | Occasionally /Occasionalmente | ... | Systematically / Sistematicamente | ... |

**f) Percentage of distinct business processes which entail PII processing / Percentuale di processi aziendali distinti che comportano l'elaborazione delle PII::**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| < 30% | ... | 30-70% | ... | >70% | ... |

**g) PII data are transferred / “exported” to other Organizations that operate under a different PII Legal Framework / I dati PII vengono trasferiti/"esportati" ad altre organizzazioni che operano in base a un quadro giuridico PII diverso:**

|  |  |  |  |
| --- | --- | --- | --- |
| Yes / Si | ... | No | ... |

|  |  |
| --- | --- |
| **h) ISO/IEC 27001 Last audit date(s) (if applicable) / Data(e) dell'ultimo audit (se applicabile):** |  |

**2)Important Note / Nota importante:**

**If applying for ISO/IEC 27701 and you are certified for ISO/IEC 27001 by another CB, you must also complete the rest of the questionnaire of this ANNEX.**

**Se si richiede la ISO/IEC 27701 e siete certificati per la ISO/IEC 27001 da un altro Organismo di Certificazione, si deve completare anche il resto del questionario di questo ALLEGATO.**

|  |  |  |
| --- | --- | --- |
| Factors related to business and organization (other than IT) / Fattori legati alL’ATTIVITA’ e all'organizzazione (DIVERSO da)  *(Required information for both standards / Richiesto per entrambi gli standard)* | | |
| 1. Complexity of the ISMS (e.g. criticality of information, risk situation of the ISMS, etc.)   **Complessità del ISMS (ad esempio criticità delle informazioni, situazione di rischio dell'ISMS, etc.)** | | Check |
| a) | Only little sensitive or confidential information, low availability requirements  Few critical assets (in terms of CIA)  Only one key business process with few interfaces and few business units involved  **Solo poche informazioni sensibili o riservate, requisiti con bassa disponibilità**  **Poche attività critiche**  **Solo un processo chiave di business con poche interfacce e poche unità coinvolte** | ... |
| b) | Higher availability requirements or some sensitive / confidential information  Some critical assets  2-3 simple business processes with few interfaces and few business units involved  **Altissima disponibilità di requisiti o informazioni sensibili / confidenziali**  **Alcuni asset critici**  **2-3 processi di business semplici con poche interfacce e poche unità coinvolte** | ... |
| c) | Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements  Many critical assets  More than 2 complex processes with many interfaces and business units involved  **Elevata quantità di informazioni sensibili o confidenziali (ad esempio salute, dati personali, assicurazioni, banche) o altissima disponibilità di requisiti**  **Molti asset critici**  **Più di 2 processi complessi con molte interfacce e unità coinvolte** | ... |
| 1. The type(s) of business performed within scope of the ISMS   **Il tipo (i) di attività svolta nel campo di applicazione del ISMS** | | |
| a) | Low risk business without regulatory requirements  **Attività a basso rischio senza requisiti normativi** | ... |
| b) | High regulatory requirements  **Requisiti normativi alti** | ... |
| c) | High risk business with (only) limited regulatory requirements  **Attività ad alto rischio con (solo) limitati requisiti normativi** | ... |
| 1. Previously demonstrated performance of the ISMS   **Prestazioni precedentemente dimostrate del Sistema di Gestione dell’informazione** | | |
| a) | Recently certified  Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system  **Recentemente certificato**  **Sistema di gestione non certificato ma pienamente attuato attraverso diversi audit e miglioramento dei cicli, tra cui audit interni documentati, riesami e sistema efficace di miglioramento continuo** | ... |
| b) | Recent surveillance audit  Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented  **Recente audit di sorveglianza**  **Sistema di gestione non certificato ma parzialmente implementato: Alcuni strumenti del sistema di gestione sono disponibili e attuati; Alcuni processi di miglioramento continuo sono attuati ma parzialmente documentati** | ... |
| c) | No certification and no recent audits  ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution)  **Nessuna certificazione e nessun audit recente Il sistema di gestione è nuovo e non del tutto stabilito (ad esempio mancano specifici meccanismi di controllo del sistema di gestione, i processi di miglioramento continuo sono non maturi, realizzazione dei processi ad hoc** | ... |

|  |  |  |
| --- | --- | --- |
| Factors related to IT environment / Fattori legati all'ambiente informatico | | |
| 1. Extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks)   **Estensione e diversità della tecnologia utilizzata nella realizzazione dei vari componenti del Sistema di gestione dell’informazione (ad esempio numero di differenti piattaforme, numero di reti segregate)** | | |
| a) | Highly standardized environment with low diversity (few IT platforms, servers, operating systems, databases, networks, etc.)  **Ambiente altamente standardizzato con bassa diversità (alcune piattaforme informatiche, server, sistemi operativi, database, reti, ecc.)** | ... |
| b) | Standardized but diverse IT platforms, servers, operating systems, databases, networks  **Ambiente standardizzato ma diverse piattaforme IT, server, sistemi operativi, database, reti** | ... |
| c) | High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications)  **Alta diversità o complessità alta di IT (es. molti diversi segmenti di reti, tipi di server o database, numero di applicazioni chiave)** | ... |

|  |  |  |
| --- | --- | --- |
| 1. Extent of outsourcing and third party arrangements used within the scope of the ISMS   **Estensione dell’esternalizzazione e accordi con terze parti utilizzate nell'ambito di attuazione del Sistema di gestione dell’informazione** | | |
| a) | No outsourcing and little dependency on suppliers, or  Well-defined, managed and monitored outsourcing arrangements  Outsourcer has a certified ISMS  Relevant independent assurance reports are available  **Nessun processo in outsourcing e poca dipendenza dai fornitori, o**  **Accordi di outsourcing ben definiti, gestiti e monitorati**  **L’outsourcer ha un sistema di gestione dell’informazione certificato**  **Sono disponibili report con aziende indipendenti** | ... |
| b) | Several partly managed outsourcing arrangements  **Diversi accordi di esternalizzazione in parte gestiti** | ... |
| c) | High dependency on outsourcing or suppliers with large impact on important business activities, or  Unknown amount or extent of outsourcing, or  Several unmanaged outsourcing arrangements  **Alta dipendenza di outsourcing o fornitori con grande impatto su importanti attività di business, o**  **quantità o estensione di outsourcing sconosciuta, o**  **Diversi accordi in outsourcing non gestiti** | ... |
| 1. Extent of information system development   **Grado di sviluppo del sistema informativo** | | |
| a) | No in-house system development  Use of standardized software platforms  **Lo sviluppo del sistema non è “in casa”**  **L'utilizzo di piattaforme software standardizzate** | ... |
| b) | Use of standardized software plat- forms with complex configuration / parameterization  (Highly) customized software  Some development activities (in-house or outsourced)  **L'utilizzo di un software standardizzato con una piattaforma di configurazione complessa / parametrizzazione**  **Software (altamente) su misura**  **Alcune attività sviluppate (in-casa o in outsourcing)** | ... |
| c) | Extensive internal software development activities with several ongoing projects for important business purpose  **Ampia attività di sviluppo software interni con numerosi progetti in corso per scopi importanti di business** | ... |
| Multi-site Information / INFORMAZIONI SUI MULTI-SITO | | |
| 1. Number of sites and number of Disaster Recovery (DR) sites   **Numero di siti e numero di siti di Disaster Recovery (DR)** | | |
| a) | Low availability requirements and no or one alternative DR site  **Requisiti di disponibilità bassi e nessuna o un sito alternativo di DR** | ... |
| b) | Medium or High availability requirements and no or one alternative DR site  **Requisiti di disponibilità media o alta e nessuna o un sito alternativo di DR** | ... |
| c) | High availability requirements e.g. 24h a day /7 day a week services  Several alternative DR sites  Several Data Centers  **Requisiti di alta disponibilità dei servizi per esempio 24 ore su 24 / 7giorni su 7**  **Diversi siti alternativi di DR**  **Diversi Data Center** | ... |
| Other / Altro | | |
| 1. Document other significant information / particularities which might affect the Certification   **Documentare altre informazioni significative / particolarità che potrebbero inficiare la certificazione** | | |
| ... | | |

**Istruzioni** / Instructions:

* **Questo modulo è da inviare sempre insieme con il Costumer Profile (F-2503 form)**
* This form is always to be send along with Organization Profile (F-2503 form)

|  |  |  |
| --- | --- | --- |
| ... |  | ... |
| **Rappresentantedell’Organizzazione**  Representative Name | **Firma**  Signature | **Data**  Date |

# - Revision History -

|  |  |  |  |
| --- | --- | --- | --- |
| Revision No | Revision Date | Nature of Change | Review and Approval |
| 0 | September 5, 2016 | Addition to F-2503 | LDK |
| 1 | October 14, 2016 | Revised as per new ISO 27006:2015. Re-formatted as per Forms 2.0 style | LDK |
| 2 | June 3, 2023 | Addition of information regarding ISO/IEC 27701 certification | VN/LDK |