QUESTIONARIO
CYBER INSURANCE

Questionario Cyber QBE

DETTAGLI DEL RICHIEDENTE

1. Ragione Sociale:

_____

2. Indirizzo completo del richiedente:

_____

3. Codice Fiscale/P.IVA:

_____

4. Sito web:

_____

5. Data di inizio dell'attività:

_____

6. Si prega di indicare il settore principale (e secondario) nel quale opera la società:

_____

DETTAGLI FINANZIARI DEL RICHIEDENTE

7. Si prega di indicare il fatturato totale della proponente e delle società per cui è richiesta la copertura assicurativa: _____

8. A quale anno si riferisce il fatturato di cui sopra: _____

9. Percentuale di fatturato proveniente dall'attività e-commerce: _____

10. Si prega di inserire la suddivisione del fatturato nella seguente tabella:

Fatturato	Ultimo esercizio	Esercizio corrente (stima)	Esercizio successivo (stima)
USA/Canada (domestico)			
USA/Canada (filiali)			
USA/Canada (export)			
Resto del mondo (USA/Canada escluso)			
Consolidato			

11. Indicare se la Contraente ha o ha avuto un fatturato verso clienti aventi sede in paesi soggetti ad embargo o sanzioni (ad esempio: Russia, Cuba, Iran, Crimea, Sudan, Myanmar, Corea del Nord, Siria, Bielorussia). Se sì, fornire dettagli:

_____

_____

Governance

12. Sono presenti delle policy riguardo la sicurezza informatica e privacy dei dati e i rischi e gli obiettivi raggiunti vengono riportati al senior management (amministratori)? SI □ NO □
13. Il management è direttamente coinvolto nella gestione dei dati sulla privacy e la sicurezza informatica? SI □ NO □
14. I dati riguardanti la sicurezza informativa e privacy vengono riferiti direttamente al senior management? SI □ NO □
15. Il senior management supporta attivamente l'importanza della sicurezza informatica e privacy dei dati? SI □ NO □
16. I dati sulla privacy e la sicurezza informatica sono identificati come dei rischi d'impresa e sono gestiti secondo delle linee guida dell'organizzazione? SI □ NO □
17. Ci sono responsabili per la sicurezza informatica e i dati riguardanti la privacy tra i membri del senior management team e partecipano attivamente alle riunioni? SI □ NO □
18. Il Senior management ha un ruolo attivo nel definire la strategia e priorità della sicurezza informatica e privacy dei dati? SI □ NO □
19. È presente un membro del board con l'incarico di supervisionare la privacy e la sicurezza? SI □ NO □

Compliance

20. Sono presenti delle procedure documentate e approvate riguardo la privacy dei dati e la sicurezza informatica? SI □ NO □
21. La compliance riguardo la privacy dei dati e la sicurezza informatica è monitorata da soggetti responsabili e specializzati? SI □ NO □
22. Vengono utilizzate delle procedure ben definite per monitorare la compliance della sicurezza informatica e la privacy dei dati ed essa viene effettuata da soggetti responsabili e specializzati? SI □ NO □
23. Esistono processi aziendali di controllo dei consensi e dell'utilizzo dei dati? SI □ NO □
24. La sicurezza informatica e la privacy dei dati è revisionata annualmente da organismi interni indipendenti (Internal Audit) oppure da organismi esterni all'azienda? SI □ NO □
25. Le attività non compliant e le eccezioni sono considerate formalmente dal management e viene effettuata un'attività di rimedio? SI □ NO □
26. Sono presenti delle certificazioni industriali attestate da organizzazioni terze (come ad esempio PCI-DSS, ISO27001, SOC 2)? SI □ NO □

Sicurezza del Personale

27. Sono presenti dei documenti riguardanti gli standard di sicurezza del personale? SI □ NO □

28. Il personale deve dare il proprio consenso ad una informativa sulla privacy e alla sicurezza informatica? SI □ NO □
29. Esistono dei corsi specifici per il personale? SI □ NO □
30. Viene effettuato un controllo sui candidati prima che essi vengano assunti? SI □ NO □
31. Le responsabilità sulla sicurezza informatica, inclusa la confidenzialità, sono comprese all'interno del contratto lavorativo? SI □ NO □
32. Gli individui appena assunti ricevono dei corsi di apprendimento e sono consapevoli delle procedure e standard adottati in azienda? SI □ NO □
33. Vengono somministrati annualmente dei corsi di aggiornamento riguardo la sicurezza, compresi gli obblighi normativi? SI □ NO □
34. Terminato il rapporto lavorativo, gli individui devono consegnare gli strumenti utilizzati durante l'attività lavorativa, e tali strumenti vengono riutilizzati o smaltiti? SI □ NO □
35. È presente un programma annuale di corsi di aggiornamento? SI □ NO □
36. Vengono svolti corsi e simulazioni su tematiche phishing? SI □ NO □
37. I corsi sono specifici per ogni ruolo? SI □ NO □
38. L'attività di efficacia e consapevolezza viene costantemente riportata e monitorata? SI □ NO □

Gestione dei Dati

39. È presente una classificazione dei dati e una procedura di gestione e smaltimento dei dati? SI □ NO □
40. Viene mantenuto un inventario dei dati? SI □ NO □
41. Il personale riceve un corso riguardo la classificazione e gestione dei dati? SI □ NO □
42. Esistono delle procedure aziendali documentate per la gestione dei dati e delle autorizzazioni (pubblicazione, condivisione, modifica)? SI □ NO □
43. I dati critici vengono criptati tramite la crittografia at rest (endpoints e cloud), in transito (attraverso la rete ed e-mail) o sui dispositivi mobili? SI □ NO □
44. Sono presenti dei tool tecnici, come ad esempio strumenti per la prevenzione della perdita dei dati? SI □ NO □
45. Le informazioni personali, finanziarie e confidenziali riguardanti l'attività aziendale vengono criptate tramite la crittografia at rest, in transito o sui dispositivi mobili? SI □ NO □

Sicurezza di Terzi

46. Sono effettuate delle valutazioni sulla sicurezza di base per le organizzazioni terze? SI □ NO □
47. Sono presenti degli accordi scritti con le organizzazioni terze principali? SI □ NO □
48. È disponibile un registro in cui vengono registrate dati di accesso delle organizzazioni terze? SI □ NO □
49. Gli organismi terzi hanno completato le autovalutazioni di sicurezza e sono in vigore termini e condizioni standard? SI □ NO □
50. È presente un registro del rischio dei terzi? SI □ NO □
51. È stata ottenuta una garanzia indipendente (SOC2, ISO27001, test di penetrazione, ecc.) sugli accordi di sicurezza delle organizzazioni terze e sono state inserite delle clausole contrattuali specifiche sulla sicurezza negli accordi? SI □ NO □
52. Gli accordi sulla sicurezza con le organizzazioni terze e compliance sono revisionati su base annuale e ogniqualvolta avvengano delle modifiche significative all'ambito dei servizi? SI □ NO □

Sicurezza Fisica e Ambientale

53. Solamente il personale e visitatori autorizzati hanno la possibilità di accedere agli strumenti informatici? SI □ NO □
54. I visitatori devono loggarsi e disconnettersi per usufruire degli strumenti informatici? SI □ NO □
55. Nelle strutture IT sono presenti controlli ambientali di base, tra cui gruppi di continuità (UPS) e aria condizionata? SI □ NO □
56. Sono presenti dei dispositivi CCTV per l'ingresso/uscita in azienda, e nelle aree comuni? SI □ NO □
57. Sono presenti delle barriere fisiche, come ad esempio dei tornelli? SI □ NO □
58. Viene fornito un badge ai visitatori per l'identificazione? SI □ NO □
59. Esistono controlli ambientali specifici, tra cui pavimentazione rialzata, soppressione degli incendi e generatori di riserva, nelle strutture IT? SI □ NO □
60. Le autorizzazioni ad accessi fisici vengo revisionate regolarmente? SI □ NO □
61. Esistono accordi di supporto per il mantenimento dei controlli ambientali, come ad esempio un contratto con terzi per la manutenzione del sistema antincendio? SI □ NO □
62. I visitatori vengono accompagnati in aree riservate dell'azienda? SI □ NO □
63. Sono presenti nei locali e nelle strutture IT in outsourcing dei controlli fisici e ambientali? SI □ NO □

Gestione Incidenti

64. È presente una procedura per gestire gli incidenti documentati? SI □ NO □
65. È presente un business continuity plan documentato? SI □ NO □
66. Esistono procedure e piani di risposta agli incidenti per ridurre l'impatto degli incidenti, per identificarne la causa e sono comunicati agli stakeholder? SI □ NO □
67. Vengono registrati tutti gli incidenti di sicurezza e vengono successivamente preparati dei corsi per evitare che si ripetano nuovamente? SI □ NO □
68. I piani di risposta agli incidenti e i piani di continuità operativa vengono esercitati a livello dirigenziale, ad esempio con esercitazioni da tavolo su base almeno annuale? SI □ NO □
69. Esistono playbook operativi di supporto per la risposta agli incidenti di sicurezza per tutte le categorie di incidenti? SI □ NO □
70. I piani di risposta agli incidenti e di continuità operativa sono esercitati a livello operativo, SI □ NO □
71. ad esempio, testando gli accordi di lavoro fuori sede, con cadenza almeno annuale? SI □ NO □
72. Esiste un supporto specialistico per gli incidenti tramite risorse interne dedicate o terze parti specializzate? SI □ NO □

Controlli degli Accessi

73. Esistono politiche e procedure documentate per il controllo degli accessi legate alla sicurezza dei dipendenti? SI □ NO □
74. E' presente una password policy? SI □ NO □
75. Gli account degli utenti sono creati sulla base del criterio *least privilege*? SI □ NO □
76. Il controllo degli accessi basato sui ruoli è applicato con una chiara giustificazione aziendale in relazione ai dati da gestire? SI □ NO □
77. Gli user accounts utilizzano un unico ID? SI □ NO □
78. Sono presenti per tutte le risorse informatiche delle password forti? SI □ NO □

79. Viene utilizzato il sistema di autenticazione a multi-fattori per gli accessi ad account amministrativi? SI □ NO □
80. E' possibile accedere da remoto ai sistemi aziendali? SI □ NO □
81. Se avete risposto SI alla domanda precedente, è richiesta la multi-factor-authentication (MFA) per poter accedere ai sistemi aziendali? SI □ NO □
82. Per gli accessi per cui non è prevista la multi-factor-authentication (MFA) esiste una documentazione che regola gli accessi da remoto? SI □ NO □
83. E' presente un registro aggiornato contenente gli accounts con accesso privilegiato? SI □ NO □
84. E' presente una piattaforma di gestione per gli account con accesso privilegiato? SI □ NO □
85. I diritti di accesso vengono rivisti su base trimestrale, compresi gli account privilegiati, per confermare che sono ancora necessari? SI □ NO □
86. L'autenticazione a multi-fattori è utilizzata per l'accesso di tutti gli user accounts e risorse informatiche? SI □ NO □

4.9 Protezione Anti-Malware

87. Gli strumenti anti-malware (inclusi software antivirus) sono schierati in tutti gli endpoints? SI □ NO □
88. Gli strumenti anti-malware vengono aggiornati automaticamente? SI □ NO □
89. Gli strumenti anti-malware sono gestiti tramite una console centrale? SI □ NO □
90. Gli strumenti anti-malware sono configurati in modo da effettuare delle scansioni periodiche? SI □ NO □
91. Gli strumenti anti-malware sono configurati in modo di poter identificare e rimuovere tutte le tipologie di malware conosciute, come Malware, Rootkits e PUAs (Potentially Unwanted Applications)? SI □ NO □
92. Le impostazioni di configurazione anti-malware possono essere modificate dal personale? SI □ NO □
93. Le porte USB sono disabilitate? SI □ NO □
94. Gli strumenti con capacità di rilevamento e risposta degli endpoint sono distribuiti su tutti gli endpoint? SI □ NO □
95. La configurazione e l'efficacia degli strumenti vengono continuamente riviste per mitigare le minacce emergenti e ridurre i falsi positivi? SI □ NO □

SI □ NO □

Sicurezza di Rete e Posta Elettronica

96. Sono utilizzate le protezioni native (integrate) fornite dai provider di servizi di posta elettronica e dai browser web? SI □ NO □
97. I PC portatili sono protetti tramite firewall personali? SI □ NO □
98. Sono presenti degli strumenti di sicurezza riguardanti la posta elettronica, per fornire una protezione contro malware ricevuti via mail, phishing e email spoofing? SI □ NO □
99. Sono disponibili degli strumenti di filtraggio di gateway che garantiscano una protezione contro siti web compromessi o sospetti? SI □ NO □
100. Le impostazioni di configurazione degli strumenti di sicurezza sono continuamente revisionate, in modo da poter identificare minacce emergenti e ridurre i falsi positivi? SI □ NO □
101. Sono presenti multipli sistemi di sicurezza, per fornire protezione in multipli livelli contro malware avanzati, phishing e malicious websites? SI □ NO □

Monitoraggio della Sicurezza

102.	Per poter utilizzare i sistemi e servizi informatici critici è necessario eseguire l'accesso?	SI	□	NO	□
103.	La data e l'ora sono incluse in tutti i logs?	SI	□	NO	□
104.	Gli audit logs sono mantenuti per almeno 90 giorni?	SI	□	NO	□
105.	Per poter utilizzare tutti i sistemi e servizi informatici (IoT e sistemi di controllo inclusi) è necessario eseguire l'accesso?	SI	□	NO	□
106.	Gli audit registrano le attività degli utenti, le eccezioni, gli eventi di sicurezza, le attività dell'amministratore di sistema e dell'operatore di sistema?	SI	□	NO	□
107.	È presente un sistema di monitoraggio per identificare accessi non autorizzati modifiche o comportamenti maliziosi?	SI	□	NO	□
108.	Viene effettuato un monitoraggio di tutte le compromissioni della sicurezza informatica e tali attività consentono di inviare alert gli amministratori della sicurezza riguardo gli eventi critici?	SI	□	NO	□
109.	Sono utilizzati sistemi di monitoraggio remoto e dei servizi di gestione in modo appropriato?	SI	□	NO	□
110.	I servizi di accesso e monitoraggio sono integrati con altre informazioni sulla sicurezza (Security Information & Event Management - SIEM)?	SI	□	NO	□

Sicurezza della Rete

111.	La rete è protetta contro connessioni esterne non autorizzate, tramite l'utilizzo di firewalls o ACLs (Access Control Lists)?	SI	□	NO	□
112.	Tutti i dati in transito, compresi quelli di autenticazione, sono criptati attraverso la rete?	SI	□	NO	□
113.	Esiste una segmentazione tra reti fidate e non fidate, ad esempio tra reti aziendali (sede centrale) e reti operative (produzione)?	SI	□	NO	□
114.	È presente il Network Access Control (NAC) nelle aree critiche della rete?	SI	□	NO	□
115.	È presente qualche forma di sistema di rilevazione delle intrusioni oppure qualche procedura per la rilevazione di accessi non autorizzati nella rete?	SI	□	NO	□
116.	Esiste una visualizzazione regolare delle regole e della configurazione del firewall?	SI	□	NO	□
117.	È presente qualche sistema di rilevazione e prevenzione nei punti strategici della rete?	SI	□	NO	□
118.	I sistemi di segnalazione delle intrusioni sono regolarmente monitorati e revisionati?	SI	□	NO	□
119.	Il Network Access Control (NAC) è implementato in tutta la rete e viene regolarmente revisionato?	SI	□	NO	□

Configurazione e Sviluppo IT

120.	Sono presenti delle procedure documentate per mantenere i sistemi e le infrastrutture?	SI	□	NO	□
121.	I servers sono costruiti e configurati seguendo un unico standard per l'intero dipartimento IT?	SI	□	NO	□
122.	È presente un inventario degli assets IT?	SI	□	NO	□
123.	Le modifiche sono formalmente gestite e vengono valutati gli impatti eventuali sulla sicurezza?	SI	□	NO	□
124.	Tutti i server sono costruiti e configurati in modo standard in tutta l'infrastruttura IT?	SI	□	NO	□

125. Il dipartimento IT è gestito centralmente, inclusa l'abilità di formattare da remoto i dispositivi mobili? SI □ NO □
126. Vengono programmati gli aggiornamenti della sicurezza per tutto il ciclo di vita dei software in uso? SI □ NO □
127. È presente una separazione logica tra i dipartimenti di sviluppo, test e produzione? SI □ NO □
128. Vengono utilizzati strumenti di gestione della configurazione per mantenere e automatizzare la distribuzione di *secure build*? SI □ NO □
129. Sono applicate in tutte le attività del dipartimento IT delle procedure di sviluppo software e sono revisionate regolarmente? SI □ NO □
130. Sono presenti delle procedure per gestire in sicurezza hardware e software end-of-life oppure non più supportati dai produttori? SI □ NO □

Backup IT e Ripristino di Emergenza

131. Esistono procedure documentate per il backup e il ripristino di sistemi e servizi critici? SI □ NO □
132. Vengono regolarmente effettuati i backups dei dati critici? SI □ NO □
133. Vengono conservate copie offsite protette di software critici? SI □ NO □
134. Vengono conservate backup offsite protetti dei dati critici? SI □ NO □
135. Vengono effettuati dei test del ripristino di backup critici? SI □ NO □
136. Vengono conservati dei files di backup anche nel momento in cui essi non sono più necessari? SI □ NO □
137. Sono presenti delle procedure documentate per i backup e sistemi di ripristino? SI □ NO □
138. Sono presenti dei piani documentati per il ripristino di dati, persi o corrotti a causa di incidenti informatici, incluso il ripristino di sistemi molto importanti? SI □ NO □
139. Vengono effettuate delle attività di pianificazione della capacità, gestione (come il bilanciamento del carico) e monitoraggio per garantire l'adeguatezza delle capacità di elaborazione e archiviazione? SI □ NO □
140. Sono conservati dei backup offline? SI □ NO □
141. Vengono effettuati dei test di ripristino di tutti i backup regolarmente? SI □ NO □
142. Vengono effettuate almeno una volta l'anno delle esercitazioni contro eventi disastrosi informatici? SI □ NO □

Gestione Tecnica delle Vulnerabilità

143. I sistemi operativi, i database e le applicazioni critiche ricevono aggiornamenti di sicurezza dal fornitore o dalla distribuzione (open source)? SI □ NO □
144. Esistono procedure documentate per l'identificazione delle vulnerabilità di sicurezza, e vengono effettuate delle classificazioni delle loro criticità? SI □ NO □
145. Tutti i sistemi operativi, i database e le applicazioni ricevono aggiornamenti di sicurezza dal fornitore o dalla distribuzione? SI □ NO □
146. Viene eseguita una scansione regolare delle vulnerabilità sui sistemi critici? SI □ NO □
147. Esistono procedure documentate per la valutazione e la mitigazione delle vulnerabilità di sicurezza (ad esempio, regolari patch di sicurezza)? SI □ NO □
148. Vengono eseguiti test di penetrazione ad hoc? SI □ NO □
149. Vengono eseguiti regolarmente test di penetrazione in tutta la struttura IT? SI □ NO □

150. Gli asset IT sono valutati in base al rischio/impatto sul business per stabilire la priorità del loro aggiornamento? SI □ NO □

Impatto sulle Attività Aziendali

151. Se dovesse accadere un incidente Cyber (ad esempio un evento di hackeraggio che impedisse di utilizzare i sistemi informatici), quanto tempo trascorrerebbe prima che si registri una perdita?

<1h □ 1h-12h □ 12h-24h □ 24h-48h □ >48h □

152. Indicare la perdita prevista giornalmente nel caso in cui un incidente Cyber dovesse accadere:

_____

6. RICHIESTE DI RISARCIMENTO

153. Negli ultimi 3 anni, il richiedente ha mai subito una violazione intenzionale della sicurezza IT, danni alla rete, interruzione dell'attività o danneggiamento del sistema? SI □ NO □

154. Se avete risposto 'SI' alla domanda precedente, si prega di fornire i dettagli, includendo la data del/dei sinistri e l'ammontare pagato o riservato da parte della compagnia di assicurazione e/o i dettagli di ogni interruzione dell'attività aziendale subita:

_____

_____

155. Se avete risposto 'SI' alla domanda precedente, quali misure sono state poste in essere per prevenire che in futuro si ripetano situazioni simili?

_____

_____

156. I dati conservati e maneggiati dal richiedente sono mai stati compromessi o trafugati? SI □ NO □

157. Se avete risposto 'SI' alla domanda precedente, si prega di fornire i dettagli, includendo la data del/dei sinistri e l'ammontare pagato o riservato da parte della compagnia di assicurazione e/o i dettagli di ogni interruzione dell'attività aziendale subita:

_____

158. Se avete risposto 'SI' alla domanda precedente, quali misure sono state poste in essere per prevenire che in futuro si ripetano situazioni simili? SI □ NO □

_____

_____

159. Il richiedente è a conoscenza di informazioni su qualsiasi fatto, circostanza, situazione, evento o transazione che possano dare luogo ad una richiesta di risarcimento o notifica di violazione dei dati? Se sì, fornire i dettagli di seguito:

_____

_____

7. ALTRE INFORMAZIONI

160. Se ci sono altre informazioni che ritenete pertinenti, vi preghiamo di fornirle di seguito:

_____

_____

_____

_____

_____

_____

_____

8. DICHIARAZIONE

Dichiaro/dichiariamo che la presente proposta è stata compilata dopo le opportune indagini e che le dichiarazioni e i dati contenuti nella presente proposta (compresi tutti gli allegati, se del caso) sono veritieri e che io/noi non abbiamo dichiarato o non abbiamo in alcun modo travisato o taciuto alcun fatto rilevante.
Mi impegno/ Ci impegniamo ad informare i sottoscrittori di qualsiasi modifica sostanziale di tali fatti, sia che si verifichi prima o dopo il perfezionamento della proposta del contratto di assicurazione.

Firma del Committente/Partner/Direttore Data

_____ _____

INFORMATIVA PRIVACY AI CONTRAENTI

1. Introduzione

QBE Europe SA/NV - Rappresentanza Generale per l'Italia (la "**Società**") la informa, in qualità di **Titolare del trattamento** (che può essere contattato all'indirizzo email: dpo@uk.qbe.com e reclami@it.qbe.com) che i dati personali relativi all'assicurato/contraente/beneficiario (l'"**Interessato**"), necessari per la prestazione dei servizi e/o l'esecuzione degli obblighi della polizza a cui la presente informativa è allegata (la"**Polizza**"), saranno trattati in conformità con la presente Informativa.

2. Chi è il titolare del trattamento?

La Società con sede secondaria in Milano, Via Melchiorre Gioia, 8 sito internet: http://www.qbeitalia.com è il **Titolare del trattamento** e può essere contattata al seguente indirizzo e-mail: dpo@uk.qbe.com o reclami@it.qbe.com.

Una lista completa dei Responsabili del trattamento nominati dalla Società può essere richiesta alla stessa con una comunicazione agli indirizzi sopra indicati.

3. Quali tipologie di Dati Personali vengono trattati dalla Società?

La **Società** tratta le seguenti tipologie di dati personali dell'Interessato (complessivamente i "**Dati Personali**"), acquisiti- anche verbalmente -direttamente presso l'**Interessato** o tramite soggetti terzi:

a) dati identificativi quali, ad esempio: nome, cognome, codice fiscale, indirizzo, telefono, mail, *etc*..;
b) categorie particolari di dati, quali dati relativi alla salute.

4. Per quali finalità vengono trattati i Dati Personali?

La **Società** tratta i **Dati Personali** per le seguenti finalità:

a) per la stipula ed esecuzione della Polizza (compresa la valutazione del rischio assicurativo effettuata dalla Società sulla base di determinate caratteristiche dell'**Interessato**); e la prestazione dei servizi connessi all'attività assicurativa e riassicurativa oggetto della Polizza (di seguito, "**Finalità Assicurative**");
b) per l'adempimento di obblighi previsti da leggi o regolamenti applicabili, nonché da disposizioni impartite dalle competenti autorità/organi di vigilanza e controllo (di seguito, "**Finalità di Legge**");
c) per lo svolgimento di attività funzionali a cessioni di azienda e di ramo d'azienda, acquisizioni, fusioni, scissioni o altre trasformazioni e per l'esecuzione di tali operazioni (di seguito, "**Finalità di Legittimo Interesse di Business**").

5. Qual è la base giuridica del trattamento?

Il trattamento dei **Dati Personali** è obbligatorio per:

a) l'esecuzione della Polizza in relazione alle **Finalità Assicurative** di cui al paragrafo 4, lettera a);
b) l'adempimento agli obblighi di legge in relazione alle **Finalità di Legge** di cui al paragrafo 4, lettera b), nei limiti previsti dalla legge;
c) il legittimo interesse della Società e delle sue controparti alla conclusione degli accordi previsti alla paragrafo 4 lettera c) in relazione alle **Finalità di Legittimo Interesse di Business**.

Il rifiuto di fornire i **Dati Personali** per le finalità indicate al paragrafo 4, lettere a) e b) avrebbe il risultato di impedire alla **Società** di concludere la **Polizza** e, se già conclusa, di proseguirne l'esecuzione. Al contrario, è possibile opporsi per motivi legittimi al trattamento per le finalità di cui al paragrafo 4 lettera c), a meno che non sia individuato un motivo legittimo prevalente della **Società**.

Il trattamento dei dati sulla salute per le **Finalità Assicurative** non è obbligatorio ed è sottoposto al consenso dell'Interessato. Tuttavia, in caso di mancato consenso, la **Società** non potrà valutare il rischio assicurativo e/o dare esecuzione alla **Polizza** e, quindi, non sarà possibile addivenire alla stipula della stessa.

6. Con quali modalità vengono trattati i Dati Personali?

I **Dati Personali** vengono trattati in forma scritta e/o su supporto magnetico, elettronico o telematico e con strumenti comunque automatizzati e, in ogni caso, in modo da garantire la sicurezza e la riservatezza dei **Dati Personali** stessi.

7. A chi possono essere comunicati i Dati Personali?

I **Dati Personali** possono essere comunicati dalla **Società** a:

d) dipendenti e collaboratori della **Società** nell'ambito delle relative mansioni e in qualità di Incaricati del trattamento;
e) soggetti terzi appartenenti alla cosiddetta "catena assicurativa" quali, ad esempio, assicuratori, coassicuratori e riassicuratori; agenti, subagenti, e mediatori di Assicurazione ; consulenti legali e periti; medici legali, fiduciari, società di servizi a cui siano affidate la gestione e/o la liquidazione dei sinistri, società volte alla fornitura di servizi connessi alla gestione del rapporto contrattuale in essere o da stipulare; organismi associativi e consortili propri del settore assicurativo; IVASS, il Ministero dello Sviluppo Economico, CONSAP e UCI ed ulteriori autorità competenti ai sensi della normativa applicabile, nell'ambito della ordinaria gestione della Polizza;
f) soggetti terzi coinvolti nello specifico rapporto di Assicurazione quali, ad esempio, contraente, assicurati, beneficiari, danneggiati, coobbligati, ecc.;
g) professionisti, consulenti, istituti di credito e società di recupero dei crediti; e
h) società terze fornitrici di servizi alla Società, quali ad esempio quelli informatici o di archiviazione.

I Suoi **Dati Personali**, in ogni caso, non saranno oggetto di diffusione.

8. I Dati Personali vengono trasferiti all'estero?

I **Dati Personali** possono invece essere comunicati e trasferiti a soggetti terzi quali, ad esempio, Società del Gruppo, controllanti, controllate e collegate, residenti in Paesi anche non appartenenti all'Unione Europea (Filippine, Stati Uniti, India). L'elenco completo e aggiornato è reperibile al seguente indirizzo: http://www.qbeitalia.com/.

Tale trasferimento avverrà in conformità con gli articoli 45 e 46 del Regolamento generale sul trattamento dei dati personali 679/2016/UE (il "**Regolamento Privacy**"). L'**Interessato** può ottenere in qualsiasi momento dalla **Società** il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali **Dati Personali**, o il luogo in cui sono stati resi disponibili.

9. Per quanto tempo verranno conservati i Dati Personali?

I **Dati Personali** raccolti per le finalità di cui alle lettere a) e c) del paragrafo 4 vengono trattati per un periodo pari alla durata della **Polizza** (ivi inclusi eventuali rinnovi) e per i 10 anni successivi al termine, risoluzione o recesso della stessa, fatti salvi i casi in cui la conservazione per un periodo successivo sia richiesta per eventuali contenziosi, richieste delle autorità competenti o ai sensi della normativa applicabile.

Al contrario, i **Dati Personali** raccolti per le finalità di cui alla lettera b) del paragrafo 4 saranno conservati per il termine previsto dalla legge.

10. Che diritti ha l'Interessato con riguardo ai suoi Dati Personali?

L'**Interessato**, con riguardo ai suoi **Dati Personali** può - tramite l'invio di una comunicazione all'indirizzo di cui al paragrafo 2 - in ogni momento esercitare i propri diritti di: (i) ottenere la conferma dell'esistenza o meno di **Dati Personali** che lo riguardano ed averne comunicazione; (ii) conoscere l'origine dei **Dati Personali**, le finalità del trattamento e le sue modalità, nonché la logica applicata al trattamento effettuato mediate strumenti elettronici; (iii) chiedere l'aggiornamento, la rettifica o - se ne ha interesse - l'integrazione dei **Dati Personal**i; (iv) ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei **Dati Personali** eventualmente trattati in violazione della legge, nonché di opporsi, per motivi legittimi, al trattamento; (v) revocare, in qualsiasi momento, il consenso al trattamento dei **Dati Personali**, senza che ciò pregiudichi in alcun modo la liceità del trattamento basata sul consenso prestato prima della revoca.

In aggiunta alle previsioni di cui al presente paragrafo, ai sensi del Regolamento Privacy, l'**Interessato** potrà avvalersi dei seguenti ulteriori diritti:

a) l'**Interessato** potrà, in qualsiasi momento nelle circostanze previste dal Regolamento Privacy (i) chiedere alla **Società** la limitazione del trattamento dei **Dati Personali**; (ii) opporsi in qualsiasi momento al trattamento dei suoi **Dati Personali**, a meno che la **Società** non abbia dei motivi legittimi prevalenti; (iii) chiedere la cancellazione dei **Dati Personali** che lo riguardano senza ingiustificato ritardo e (iv) ottenere la portabilità del dati che lo riguardano;
b) l'**Interessato** avrà il diritto di proporre Reclamo al Garante per la Protezione dei Dati Personali ove ne sussistano i presupposti.

11. Come contattare il titolare del trattamento?

Qualora l'**Interessato** avesse dei dubbi o perplessità inerenti la presente Informativa privacy o volesse esercitare i diritti previsti dalla presente informativa, può contattare la **Società** ai seguenti indirizzo mail: dpo@uk.qbe.com o reclami@it.qbe.com.

La **Società** ha nominato un responsabile della protezione dei dati personali (il "**DPO**") ai sensi dell'articolo 37 del Regolamento Privacy, contattabile al seguente indirizzo email: dpo@uk.qbe.com, o al seguente indirizzo postale: QBE European Operations, Plantation Place, 30 Fenchurch Street, London.

12. Modifiche e aggiornamenti

La presente Informativa è valida sin dalla data di efficacia. La **Società** potrebbe tuttavia con un previo preavviso apportare modifiche e/o integrazioni a detta informativa, anche quale conseguenza dell'inizio dell'efficacia del Regolamento Privacy e di eventuali successive modifiche e/o integrazioni normative.

Milano 01.01.2019

QBE Europe SA/NV

Rappresentanza Generale per l'Italia

***

Consenso al trattamento dei dati

Presa visione dell'Informativa sul trattamento dei dati personali, dichiaro di essere consapevole che il trattamento dei dati personali anche relativi alla mia salute eventualmente forniti da parte di QBE Europe SA/NV in qualità di **Titolare del trattamento** è necessario per l'adempimento delle **Finalità Assicurative** di cui all'Informativa sul trattamento dei dati personali e, pertanto, presto il consenso a tale trattamento.

Il Contraente _____