Modello Organizzativo Privacy

Titolo	Modello Organizzativo Privacy
Data	23/11/2018
Versione	1.0

INDICE

1. Finalità

Il Regolamento in materia di protezione dei dati personali (UE) n. 2016/679 (nel seguito, "**RGPD"**) enuclea il principio di *"accountability"* ossia di responsabilizzazione dei soggetti che pongono in essere attività di trattamento di Dati personali.

A tale riguardo, l'art. 24 RGPD prevede che il Titolare del trattamento adotti misure tecniche ed organizzative adeguate ed efficaci al fine di garantire che il trattamento dei Dati personali abbia luogo in conformità alle Leggi sulla protezione dei dati applicabili.

A tal fine Burger King Restaurants Italia S.r.l. ha ritenuto necessario adottare il presente Modello Organizzativo Privacy (nel seguito, anche il **"Modello Organizzativo"** o il "**Modello**") al fine di specificare i presidi organizzativi e di processo di cui si è dotata per garantire una tutela effettiva ed efficace dei Dati personali di cui è Titolare del Trattamento.

2. Ambito di applicazione

Il presente Modello Organizzativo si applica agli amministratori, dirigenti, dipendenti, collaboratori, Responsabili del trattamento dei dati, fornitori, consulenti e ad ogni altro soggetto terzo che effettua operazioni di trattamento di Dati personali di cui la Società è Titolare del trattamento.

3. Definizioni

Ai fini del presente Modello Organizzativo, i termini e le espressioni definite avranno il significato nel seguito indicato. Le espressioni al singolare manterranno lo stesso significato al plurale, ove il contesto lo richieda.

Si riportano nel seguito le definizioni rilevanti ai fini della presente Procedura:

Atto di Nomina o Nomina	indica l'atto di nomina di volta in volta adottato dal Titolare volto a regolamentare il Trattamento dei dati personali effettuato da parte dei Responsabili del trattamento. Tale Nomina costituisce parte integrante e sostanziale del presente Modello.
Autorità	indica l'Autorità Garante per la Protezione dei Dati personali.

Autorizzati	indica i dipendenti della Società autorizzati dal Titolare a compiere operazioni di trattamento nell'esercizio delle funzioni agli stessi affidate.
Cancellazione dei Dati personali	indica la distruzione definitiva – fisica o tecnica – idonea a rendere non più recuperabili mediante gli ordinari mezzi disponibili in commercio le informazioni contenute in un supporto elettronico e/o cartaceo.
Consenso dell'Interessato	indica qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati personali che lo riguardano siano oggetto di trattamento.
Data Breach	indica una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali oggetto di trattamento.
Data Breach Policy	indica la Procedura adottata dalla Società al fine di disciplinare le opportune modalità di gestione del Data Breach.
Data Manager	indica i dipendenti designati direttamente dal Titolare che, nello svolgimento delle proprie funzioni e nei limiti dei poteri loro attribuiti, sono deputati alla gestione e al monitoraggio dei Trattamenti effettuati nell'ambito della propria attività.

Dati personali	indica qualsiasi informazione riguardante una persona fisica identificata o identificabile e che possa fornire dettagli sulle sue caratteristiche fisiche, le sue abitudini, il suo stile di vita, lo stato di salute, l'orientamento politico, la situazione economica, etc.
Destinatari	indica gli amministratori, i dirigenti, i dipendenti, i collaboratori, i Responsabili del trattamento dei dati, i fornitori e i soggetti terzi che effettuano operazioni di trattamento dei dati di cui la Società è Titolare e nei confronti dei quali trova applicazione il presente Modello e le relative Procedure che formano parte integrante e sostanziale del Modello.
Informativa	indica le informative ai sensi degli artt. 13 e 14 del RGPD che il Titolare rende di volta in volta in favore degli interessati. Tali informativo costituiscono parte integrante e sostanziale del presente modello.
Interessato	indica la persona fisica a cui si riferiscono i Dati personali oggetto di trattamento.
Leggi sulla protezione dei dati	indica tutte le leggi e i regolamenti, inclusi ma non limitati al Regolamento (UE) 2016/679 in materia di protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione dei dati (RGPD) e al Codice in materia di protezione dei Dati personali ex D.lgs. 196/2003 e successive modifiche (Codice Privacy) nonché provvedimenti di volta in volta in vigore che sono applicabili al Trattamento dei Dati personali.

Modello Organizzativo Privacy o Modello	indica il presente Modello organizzativo adottato dalla Società al fine di garantire la corretta gestione e implementazione dei presidi previsti dalle Leggi sulla protezione dei dati. Costituiscono parte integrante e sostanziale del presente Modello le Procedure e il Registro dei Trattamenti.
Paese terzo	indica un paese esterno allo Spazio Economico Europeo.
Privacy Officer	indica la funzione individuata dal Titolare che sovraintende all'implementazione e all'aggiornamento dei presidi previsti dalle Leggi sulla protezione dei dati.
Procedura	Si indicano le policy e procedure adottate dalla Società al fine di regolamentare i diversi aspetti legati al trattamento dei Dati personali. A mero titolo esemplificativo, rientrano nella definizione di Procedura: la Data Breach policy, la Procedura per l'esercizio dei diritti degli Interessati, la Data Retention Policy e il Regolamento sull'utilizzo degli strumenti informatici. Le Procedure formano parte integrante e sostanziale del presente Modello.
Procedura per l'esercizio dei diritti degli Interessati	indica la procedura adottata dal Titolare al fine di disciplinare le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di Trattamento di Dati personali di cui Burger King Restaurants Italia S.r.l. è Titolare al fine di agevolare e garantire l'esercizio dei Diritti degli Interessati.

Procedura sulla conservazione dei Dati Personali o *Data Retention Policy*	indica la procedura volta a illustrare le linee guida che la Società ha inteso adottare in materia di conservazione dei Dati personali e garantire che tali prescrizioni, nonché i diritti di cancellazione dei Dati personali esercitati dagli Interessati, siano pienamente rispettati.
Registro dei Trattamenti	indica il presidio che la Società, ai sensi dell'art. 30 RGPD, ha implementato al fine di mappare le operazioni di trattamento dei Dati personali di cui è Titolare del trattamento dei dati.
Responsabile del trattamento dei dati	indica l'entità esterna alla Società che tratta Dati personali per conto del Titolare del trattamento dei dati.
RGPD	indica il Regolamento Generale sulla protezione dei dati n. 2016/679.
Titolare del trattamento dei dati o il Titolare	indica l'entità che determina le finalità e i mezzi di trattamento dei Dati personali, in questo caso Burger King Restaurants Italia S.r.l., con sede legale in Strada 1, palazzo F4 Milanofiori 20090, Assago (MI).
Trattamento	indica qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione

WP29	Indica il Gruppo Articolo 29 ossia un organismo consultivo indipendente composto da un rappresentante delle varie autorità nazionali, dal Garante Europeo della protezione dei dati, nonché da un rappresentante della Commissione Europea.

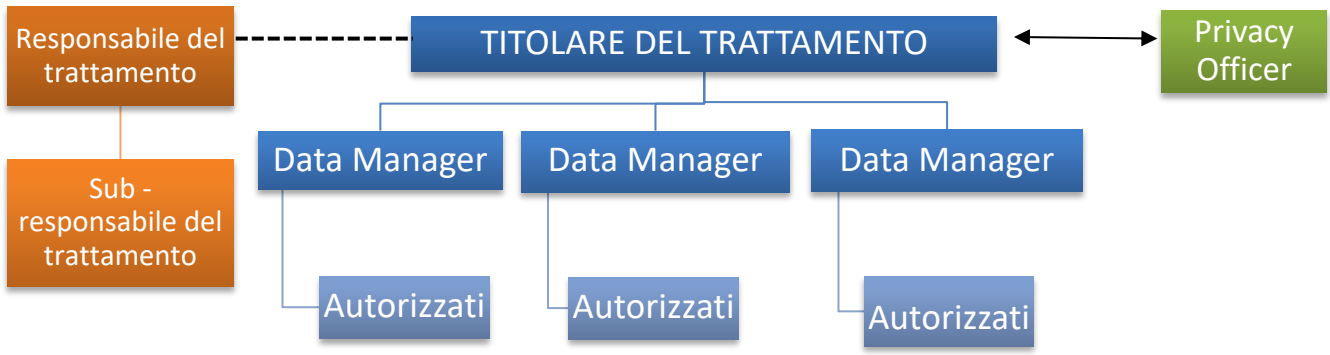
4. Ruoli e responsabilità

Il Modello Organizzativo Privacy di cui si è dotata la Società si articola su diversi livelli, riconoscendo poteri e relative responsabilità in capo a diversi soggetti:

- **il Titolare del trattamento** è il soggetto che determina le finalità e i mezzi del Trattamento dei Dati personali. Il Titolare del trattamento è Burger King Restaurants Italia S.r.l. Al Titolare del trattamento spetta il compito di adottare le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il Trattamento dei Dati personali sia effettuato conformemente alle Leggi sulla protezione dei dati. In particolare, il Titolare è chiamato, a titolo esemplificativo e non esaustivo, a:
  - Adottare le soluzioni di *privacy by design* e *privacy by default;*
  - Aggiornare il Registro dei trattamenti;
  - Predisporre le Informative relative al Trattamento dei Dati personali;
  - Predisporre ogni adempimento organizzativo necessario per garantire agli Interessati l'esercizio dei diritti;
  - Disporre l'adozione dei provvedimenti imposti dall'Autorità;
  - Effettuare la valutazione d'impatto ai sensi dell'Art. 35 RGPD;
  - Consultare l'Autorità nei casi e secondo le modalità previste dall'Art. 36 RGPD;
  - Nominare i Responsabili del trattamento.
- **Il Privacy Officer** è il soggetto che è chiamato a supervisionare e a sovrintendere il rispetto del Modello Organizzativo Privacy da parte dei Destinatari. Nell'espletamento delle sue funzioni, il Privacy Officer deve assistere il Titolare nell'attuazione delle Procedure, fungendo altresì da punto di contatto per gli Interessati e i Destinatari.
- **I Data Manager** sono i soggetti designati direttamente dal Titolare che, nello svolgimento delle proprie funzioni e nei limiti dei poteri loro attribuiti, sono deputati alla gestione e al monitoraggio dei Trattamenti effettuati nell'ambito della propria attività.

- **Gli Autorizzati al trattamento** sono tutti i soggetti che effettuano operazioni di trattamento di Dati personali, ivi inclusi i dipendenti e collaboratori che operano a qualsiasi titolo sotto la diretta autorità e secondo le istruzioni impartite dal Titolare e /o del Data Manager gerarchicamente superiore.
- **I Responsabili del trattamento** sono i soggetti terzi, esterni all'organizzazione della Società, che effettuano per conto e sotto le istruzioni del Titolare le operazioni di trattamento dei dati di cui la Società è Titolare. I Responsabili del trattamento devono essere nominati mediante atto di nomina in conformità alle prescrizioni di cui all'art. 28 RGPD.
- **I Sub-responsabili del trattamento** sono i soggetti terzi, esterni all'organizzazione della Società, nominati dal Responsabile del trattamento mediante apposito atto di nomina che impone al Sub-responsabile gli stessi obblighi in materia di protezione dei dati contenuti nell'atto di nomina a responsabile esterno del trattamento.

4.1 Flow Chart Data Protection Governance



5. Liceità

I Trattamenti effettuati dalla Società avvengono esclusivamente nel rispetto dei criteri di liceità individuati ai sensi dell'art. 6 del RGPD.

In particolare, il trattamento è lecito solo e nella misura in cui ricorra almeno una delle seguenti condizioni:

a) L'Interessato ha espresso il **consenso al trattamento** dei propri Dati personali per una o più specifiche finalità;

b) Il trattamento è necessario **all'esecuzione di un contratto di cui l'Interessato è parte** o all'esecuzione di **misure precontrattuali** adottate su richiesta dello stesso;
c) Il trattamento è necessario **per adempiere un obbligo legale** al quale è soggetto il Titolare;
d) Il trattamento è necessario **alla salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;**
e) Il trattamento è necessario per **l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri** di cui è investito il Titolare;
f) Il trattamento è necessario per il perseguimento del **legittimo interesse** del Titolare, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei Dati personali, in particolare se l'Interessato è un minore.

A tal riguardo i Destinatari sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di Trattamento di Dati Personali, la sussistenza di almeno uno dei requisiti di liceità sopra indicati. In caso di dubbi relativi alla liceità del trattamento o in merito alla base giuridica da utilizzare in relazione allo specifico trattamento i Destinatari possono rivolgersi al Privacy Officer

5.1 Consenso

Nel caso in cui il Trattamento dei Dati personali si fondi sul consenso al Trattamento espresso dall'Interessato, il Titolare deve essere in grado di dimostrare che l'Interessato abbia effettivamente fornito il suo consenso.

Il consenso reso dagli Interessati deve essere:

- Informato: ossia preceduto da adeguata informativa;
- Libero: ossia senza condizionamenti o vincoli;
- Specifico: ossia riferibile ad una singola finalità;
- Inequivocabile: ossia deve risultare certo che l'Interessato lo abbia prestato;
- Espresso: ossia non deve risultare dal silenzio o inattività dell'Interessato.

Nel caso in cui il consenso sia fornito nel quadro di una dichiarazione scritta riguardante anche altri temi, la richiesta di consenso dovrà essere presentata in maniera chiaramente distinguibile dagli altri temi, in una forma comprensibile e facilmente accessibile, con un linguaggio chiaro e semplice. È necessario altresì prevedere dei meccanismi che consentano all'Interessato di poter revocare in qualsiasi momento il consenso precedentemente prestato. La revoca del consenso non compromette la liceità del Trattamento sulla base del consenso prestato precedentemente.

ESEMPI:
I) Iscrizioni alle newsletter: il Titolare deve adeguatamente informare gli Interessati e raccogliere il consenso specifico degli Interessati per poter effettuare operazioni di trattamento dei dati personali per finalità di marketing diretto.
Tips: *è necessario che non siano pre-flaggate le checkbox relative alla raccolta del consenso per finalità di marketing diretto.*

A tal riguardo i Destinatari sono tenuti ad assistere il Titolare in sede di raccolta del consenso da parte degli Interessati e di relativa conservazione dello stesso. Gli Autorizzati e i Data Manager, ove nominati, sono, inoltre, tenuti ad assistere il Titolare affinché lo stesso possa garantire il diritto di revoca del consenso eventualmente esercitato dagli Interessati nei confronti del Titolare.

5.2 Legittimo interesse

Nel caso in cui il Titolare intenda fondare il Trattamento dei Dati personali sul legittimo interesse di cui è portatore, è necessario che il Titolare effettui **preliminarmente** un **test comparativo** atto a verificare la liceità del Trattamento medesimo. L'anzidetto test comparativo consta delle seguenti fasi:

a) **Purpose Test:** è necessario, in primo luogo, stabilire se l'interesse perseguito dal Titolare sia legittimo. Pertanto, tale interesse è conforme alle Leggi sulla protezione dei dati applicabili, qualora sia sufficientemente concreto e/o reale, e non meramente teorico.
b) **Necessity Test:** è necessario, in secondo luogo, che il Titolare stabilisca se il Trattamento dei Dati personali sia necessario al fine di perseguire l'interesse aziendale legittimo, verificando se il trattamento sia proporzionato ed adeguatamente mirato al raggiungimento dei suoi scopi. A tale riguardo è altresì necessario verificare se possano essere utilizzati altri mezzi, meno invasivi, per raggiungere tale scopo.
c) **Balancing Test:** è necessario, in terzo luogo, effettuare una comparazione tra il legittimo interesse di cui è portatore il Titolare e i diritti o gli interessi fondamentali dell'Interessato. Tale valutazione deve necessariamente tenere conto dei seguenti indici:

- L'interesse del Titolare,
- Le conseguenze derivanti da un eventuale mancato Trattamento;
- Il carattere sensibile dei dati oggetto di eventuale trattamento;
- La posizione dell'Interessato rispetto a una posizione dominante del Titolare (e.g. dipendente/datore di lavoro);

- Le modalità con cui i Dati personali sarebbero trattati;
- Le conseguenze derivante da tale tipologia di trattamento sui diritti e/o gli interessi fondamentali dell'Interessato
- Le ragionevoli aspettative dell'Interessato;
- Le conseguenze negative del trattamento sull'Interessato rispetto al beneficio auspicato.

Nel caso in cui all'esito delle predette valutazioni emerga che il legittimo interesse del Titolare prevale sugli interessi degli Interessati, il Titolare dovrà informarli in merito alle motivazioni per le quali il Titolare ha ritenuto di essere portatore di un interesse legittimo, i presidi adottati e le ragioni poste a fondamento della prevalenza degli interessi del Titolare su quelli dell'Interessato.

Nel caso in cui all'esito del test comparativo emerga la permanenza di conseguenze significative sull'Interessato, le operazioni di trattamento dei dati non potranno fondarsi sull'interesse legittimo del Titolare ma dovrà essere utilizzata una differente base giuridica che legittimi il Trattamento dei Dati personali.

In ogni caso, il Titolare è tenuto a documentare per iscritto il test comparativo, avendo cura di archiviare la documentazione inerente al bilanciamo effettuato e ai relativi esiti. A tale riguardo il Privacy Officer, nonché il Data Manager coinvolto nel Trattamento, ove nominato, e/o gli Autorizzati sono tenuti ad assistere il Titolare nell'espletamento del test comparativo. Il Privacy Officer è tenuto a conservare, sotto la sua responsabilità, tutte la documentazione inerente, conseguente ed accessoria al test comparativo.

ESEMPI:
I) soft spam: è configurabile un legittimo interesse del Titolare ad inviare, mediante posta elettronica, comunicazioni informative ai clienti relativamente a prodotti e/o servizi già acquistati ovvero a prodotti e/o servizi simili a quelli già acquistati.
Tips: *è necessario informare adeguatamente gli Interessati che i loro dati personali saranno trattati per tale finalità, riconoscendo agli stessi la possibilità di opporsi al trattamento.*

6. Trasparenza

Il Titolare può raccogliere e effettuare operazioni di Trattamento dei Dati personali solo nella misura in cui il Trattamento sia corretto e legittimo. In particolare, il RGPD e le raccomandazioni formulate dal WP29 pongono a carico del Titolare un obbligo di trasparenza nei confronti degli Interessati che trova applicazione tutte le volte in cui il Titolare rilascia l'informativa agli Interessati.

In particolare, l'Informativa resa agli Interessati deve essere **concisa, trasparente, intellegibile e facilmente accessibile**, con linguaggio semplice e chiaro.

Le Informative rese agli Interessati devono contenere almeno le seguenti informazioni:

- Identità e dati di recapito del Titolare e, ove applicabile, del rappresentante del Titolare e del RPD;
- Le categorie di Dati personali raccolti e trattati, nonché la fonte da cui sono stati raccolti;
- Le finalità del Trattamento, nonché la base giuridica del Trattamento;
- Gli eventuali destinatari o le eventuali categorie di destinatari dei Dati personali;
- L'intenzione del Titolare di trasferire i Dati personali a paesi o organizzazioni internazionali terzi e l'esistenza o l'assenza di una decisione di adeguatezza da parte della Commissione Europea, ovvero il riferimento ad adeguate o idonee tutele, nonché i mezzi per ottenere una copia di tali dati o il luogo ove sono stati resi disponibili.
- Il periodo di conservazione dei Dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- L'esistenza dei seguenti diritti in capo all'Interessato:
  - Diritto di accesso,
  - Diritto di rettifica,
  - Diritto di cancellazione
  - Diritto alla limitazione del trattamento,
  - Diritto di opporsi al trattamento,
  - Diritto alla portabilità dei dati,
  - Diritto di presentare reclami all'Autorità.
- Nel caso in cui il Trattamento si fondi sul Consenso dell'Interessato, è necessario informare quest'ultimo della possibilità di revocare il consenso precedentemente prestato in qualsiasi momento, senza pregiudicare la liceità del trattamento basato sul consenso prestato prima della revoca;
- Se la comunicazione di Dati personali è un obbligo legale o contrattuale ovvero un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i Dati personali, nonché le possibili conseguenze della mancata comunicazione dei Dati personali;
- L'esistenza di decisioni automatizzate tra cui la profilazione e, in tal caso, informazioni significative sulla logica adottata e la rilevanza e le conseguenze di tale trattamento per l'Interessato.

- Chi contattare in caso di domande e/o richieste di accesso.

Nel caso in cui la base giuridica del Trattamento sia il legittimo interesse del Titolare, occorre che l'Informativa rechi l'indicazione di tali interessi.

Il Titolare, nel redigere l'informativa sulla protezione dei Dati personali deve farsi assistere dal Privacy Officer.

A tal riguardo i Destinatari sono incaricati della corretta diffusione delle Informative in favore degli interessati. In caso di nuove operazioni di Trattamento i Data Manager di riferimento, ove nominati, e/o gli Autorizzati sono tenuti a coinvolgere il al Privacy Officer e/o il Titolare al fine di verificare che l'Informativa precedentemente resa sia coerente con il nuovo trattamento che si intende effettuare e se vi sia o meno la necessità di informare nuovamente l'Interessato.

7. Nomina dei Responsabili del trattamento dei dati

Il Titolare si impegna a trasferire i Dati personali nei confronti di soggetti terzi che effettuano operazioni di Trattamento dei dati per conto del Titolare stesso.

A tale riguardo, tutte le volte in cui un soggetto terzo effettui operazioni di Trattamento di Dati personali per conto e su istruzione documentata del Titolare, quest'ultimo provvede a nominare il soggetto terzo mediante Atto di Nomina a Responsabile esterno del trattamento ai sensi dell'art. 28 RGPD.

Nel caso in cui il soggetto terzo nominato Responsabile esterno del trattamento si avvalga di un altro responsabile, il Titolare provvede a rilasciare autorizzazione scritta al responsabile esterno del trattamento.

L'elenco completo dei soggetti terzi nominati in qualità di responsabili esterni del trattamento e degli eventuali sub-responsabili è disponibile presso il Privacy Officer.

Per la gestione del Trattamento dei Dati personali effettuato da parte di soggetti terzi per conto del Titolare la Società ha adottato dei format di Atti di Nomina.

A tal riguardo, gli Autorizzati e i Data Manager, ove nominati, ogni qualvolta vi sia la necessità di provvedere alla nomina di soggetti terzi quali Responsabili del trattamento sono tenuti ad assistere il Privacy Officer e/o il Titolare al fine di garantire la corretta implementazione di tale presidio.

8. Trasferimento dei Dati personali verso Paesi Terzi

Il trasferimento di Dati personali oggetto di un Trattamento o destinati ad essere oggetto di un Trattamento dopo il trasferimento verso un Paese terzo può avvenire solo qualora ricorra almeno una delle seguenti condizioni:

(A) il Paese terzo abbia ricevuto da parte della Commissione Europea **una decisione di adeguatezza**;

(B) il Titolare può trasferire Dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito **garanzie adeguate** e a condizione che gli Interessati dispongano di diritti azionabili e mezzi di ricorso effetti. Possono costituire garanzie adeguate, a titolo esemplificativo:

- le norme vincolanti d'impresa;
- le clausole tipo di protezione dei dati adottate dalla Commissione Europea;
- le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione Europea;
- un codice di condotta ex art. 40 RGPD;
- un meccanismo di certificazione approvato ai sensi dell'art. 42 RGPD.

***Attualmente**, i seguenti paesi hanno ricevuto una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 25, comma 6 Direttiva 95/46/CE:*

- *Andorra*
- *Argentina*
- *Australia*
- *Canada*
- *Faer Oer*
- *Israele*
- *Jersey*
- *Nuova Zelanda*
- *Uruguay*
- *Guernsey*

UE – USA

Il Privacy Shield fra UE e USA è un meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea, al fine di tutelare la riservatezza dei dati personali dei cittadini europei in caso di trasferimento oltreoceano a scopo commerciale.

Tips: *è necessario verificare preliminarmente se il soggetto terzo americano risulti certificato all'interno della c.d. Privacy Shield List consultando il sito: https://www.privacyshield.gov/list*

A tal riguardo i Destinatari sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di trasferimento di Dati Personali, la sussistenza di almeno uno dei requisiti sopra indicati. In caso di dubbi relativi alla possibilità di trasferire tali dati verso paesi terzi devono rivolgersi al Privacy Officer.

9. Principio di proporzionalità, minimizzazione dei dati e limitazione della conservazione

Possono essere raccolti e trattati solo i Dati personali rilevanti, non oltre la finalità specifica del Trattamento. Pertanto, in caso di raccolta di Dati personali è necessario chiedersi "Sono necessari questi Dati personali per conseguire la mia finalità legittima? Posso conseguirla senza?".

Ove possibile, i dati dovranno essere trattati in forma anonimizzata o pseudonomizzata.

Il Titolare e i Destinatari trattano i Dati personali esclusivamente per le finalità indicate al momento della raccolta dei Dati personali. Nel caso in cui le finalità del trattamento fossero oggetto di modifica è necessario ottenere, ove necessario, il consenso da parte dell'Interessato per il perseguimento delle nuove finalità ovvero verificare se il perseguimento delle nuove finalità sia ammesso dalla normativa applicabile. I Destinatari sono tenuti a consultare il Privacy Officer per ottenere maggiori informazioni e supporto nello stabilire la legittimità delle finalità, su come documentarla e ottenere l'ulteriore consenso degli Interessati.

Fermo quanto precede, i Destinatari trattano i Dati personali per il **tempo strettamente necessario a conseguire gli scopi per cui i Dati personali sono stati raccolti,** a meno che obblighi legali prevalenti impongano periodi di conservazione più lunghi o più brevi. I Dati personali non più utilizzati devono essere distrutti o anonimizzati.

A tale scopo, il Titolare ha provveduto ad adottare la Procedura sulla conservazione dei Dati personali (i.e. *Data Retention Policy*), di cui all'Allegato 1, finalizza all'individuazione di precisi limiti temporali nella conservazione delle varie tipologie e categorie di dati (in ossequio al principio della "limitazione della conservazione del dato" sancito dal RGPD), nonché i soggetti responsabili dei processi di cancellazione e anonimizzazione dei Dati personali. A tale ultimo riguardo, per garantire la conformità al predetto principio sono stati implementati dei sistemi di archiviazione configurati in modo tale da garantire la cancellazione completa o l'anonimizzazione dei Dati personali, oltre che una revisione periodica di tutti i sistemi di archiviazione contenenti Dati personali.

10. Procedura di gestione delle violazioni dei dati

Un Data Breach è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati personali oggetto di trattamento.

Non tutte le violazioni della sicurezza rientrano nella definizione di Data Breach. Affinché si configuri un Data Breach la violazione deve **comportare un rischio per i diritti e le libertà delle persone.**

Ciò significa che tale violazione deve essere suscettibile di avere un effetto significativo e dannoso sugli individui, ad esempio, causare discriminazione, danni alla reputazione, perdita finanziaria, perdita di riservatezza o qualsiasi altro significativo svantaggio economico o sociale. Si rende quindi necessario effettuare una valutazione caso per caso al fine di verificare se sia occorso o meno un Data Breach.

Al fine di garantire una maggiore comprensione, indichiamo nel seguito alcuni esempi di incidenti di sicurezza che potrebbero comportare un Data Breach:

- ✓ Perdita di backup contenente Dati personali;
- ✓ Accesso a banche dati da parte di soggetti non autorizzati;
- ✓ Attacco Hacker al sistema informatico;
- ✓ Furto o smarrimento di computer, laptop, devices elettronici portatili, chiavette USB, smartphones/iPad aziendali;
- ✓ Ransomware;
- ✓ Phishing.

In forza del principio di *accountability,* ossia di responsabilizzazione, che informa la normativa in materia di protezione dei Dati personali, il Titolare ha implementato la *Data Breach Policy,* di cui all'Allegato 2*,* ossia una Procedura tesa ad individuare le azioni necessarie da implementare tutte le volte in cui sia occorsa una violazione dei Dati personali ovvero vi sia una sospetta violazione dei Dati personali.

I Destinatari sono tenuti a segnalare ogni potenziale violazione dei dati di cui possano venire a conoscenza, contattando tempestivamente il Privacy Officer e/o inviando un'e-mail a privacybkri@burgerking.it .

11. Procedura per l'esercizio dei diritti degli Interessati

Il RGPD consente agli Interessati di richiedere al Titolare di:

- accedere ai propri dati e ricevere informazioni relative ai trattamenti effettuati dal Titolare (Art. 15 RGPD);
- ottenere la rettifica dei Dati personali inesatti che lo riguardano (Art. 16 RGPD);
- richiedere la cancellazione dei propri dati (Art. 17 RGPD);
- ottenere, ove consentito, la limitazione del trattamento (Art. 18 RGPD);

- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano (Art. 20 RGPD);
- opporsi in qualsiasi momento al trattamento dei Dati personali che lo riguardano (Art. 21 RGPD);
- non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla persona (Art. 22 RGPD).

Da ultimo, il RGPD conferisce agli Interessati il diritto di proporre reclamo all'Autorità ai sensi dell'art. 77 RGPD nel caso in cui l'Interessato ritenga che il trattamento che lo riguardi violi il RGPD.
Al fine di favorire e garantire il corretto ed efficace esercizio dei diritti da parte degli Interessati, il Titolare ha predisposto la Procedura per l'esercizio dei diritti dell'Interessato, di cui all'Allegato 3, finalizzata ad individuare le modalità attraverso le quali gli Interessati possono esercitare agevolmente i loro diritti. L'anzidetta Procedura individua altresì i soggetti deputati alla gestione delle richieste avanzate dagli Interessati e le relative modalità e tempistiche di gestione delle richieste.
A tal riguardo, i Destinatari sono tenuti, in conformità con quanto previsto dalla Procedura per l'esercizio dei diritti degli interessati, ad assistere il Titolare al fine di consentire allo stesso la corretta gestione delle richieste presentate dagli Interessati.

12. Registro dei Trattamenti

Il Titolare ha provveduto ad implementare il Registro dei Trattamenti finalizzato a mappare le diverse operazioni di trattamento dei Dati personali effettuate sotto la responsabilità dei Data Manager.
Il Registro dei Trattamenti è un utile strumento per la completa ricognizione e valutazione dei Trattamenti effettuati e, pertanto, è finalizzato anche all'analisi del rischio e ad una corretta pianificazione dei Trattamenti.

Il Titolare è responsabile alla corretta tenuta del Registro dei Trattamenti, nonché alla sua integrazione ed aggiornamento. A tale riguardo i Data Manager di riferimento, ove nominati e/o gli Autorizzati sono tenuti ad assistere il Titolare al fine di espletare le predette funzioni inerenti la tenuta del Registro dei trattamenti.

Ai sensi dell'Art. 30 RGPD il Registro dei Trattamenti contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del Titolare e, ove applicabile, del Contitolare del trattamento, del rappresentante del Titolare e del RPD; b) ***le finalità*** *del trattamento; c) una descrizione delle* ***categorie di Interessati*** *e delle* ***categorie di dati personali*** *d) le* ***categorie di destinatari*** *a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile,* ***i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale****, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, nonché la documentazione delle garanzie adeguate, ove applicabile; f) ove possibile,* ***i termini*** *ultimi previsti* ***per la cancellazione*** *delle diverse categorie di dati; g) ove possibile, una* ***descrizione generale delle misure di sicurezza tecniche e organizzative*** *implementate.*

13. Valutazione d'impatto sulla protezione dei dati

In linea generale, in forza del principio di ***privacy by design*** è necessario che il Titolare, al fine di tutelare i diritti e le libertà degli Interessati con riguardo al Trattamento dei Dati personali, attui adeguate misure tecniche e organizzative fin al momento della progettazione del Trattamento stesso.

Tutte le volte in cui un determinato tipo di Trattamento dei Dati personali possa presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei Dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

A titolo esemplificativo: un rischio elevato potrebbe presentarsi qualora il trattamento comporti:
- l'uso di nuove tecnologie;
- la profilazione degli Interessati;
- il trattamento di dati sensibili o aventi carattere altamente personale;
- il monitoraggio sistematico degli Interessati (ivi inclusa la sorveglianza);
- il trattamento di dati relativi a Interessati vulnerabili

La valutazione d'impatto è tesa a descrivere il Trattamento dei Dati personali, valutandone la necessità e la proporzionalità, nonché a contribuire alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal Trattamento stesso, valutando detti rischi e determinando le misure per affrontarli.

La valutazione d'impatto deve essere effettuata fin dalla fase di progettazione del Trattamento, benché alcune operazioni di trattamento non siano ancora note.

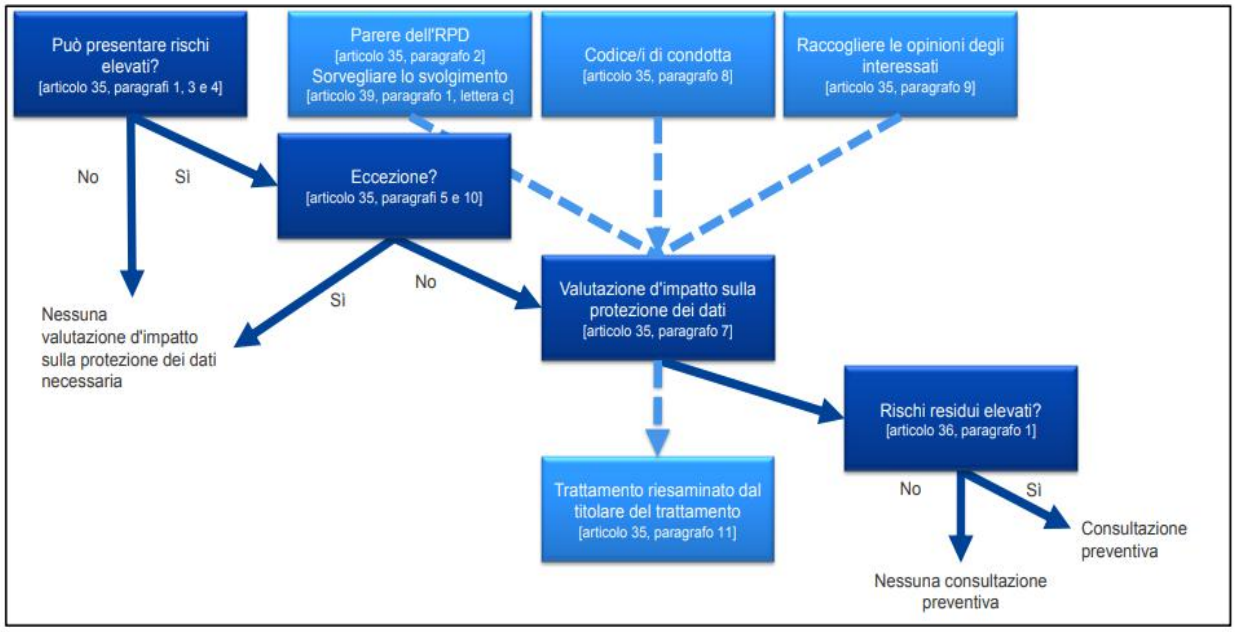
Nel caso in cui ricorra la necessità e/o l'opportunità di effettuare una valutazione di impatto, il Privacy Officer e i Destinatari sono tenuti ad assistere il Titolare fornendo tutte le informazioni necessarie ai fini della valutazione.
Il Privacy Officer è tenuto a conservare, sotto la sua responsabilità, tutta la documentazione inerente, conseguente ed accessoria alla valutazione d'impatto.

Al fine di effettuare una valutazione d'impatto, il Titolare è tenuto ad effettuare:

- una descrizione sistematica dei Trattamenti previsti e delle finalità del Trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità perseguita;
- una valutazione dei rischi per i diritti e le libertà degli Interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei Dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli Interessati e delle altre persone in questione.

Nel caso in cui, all'esito della valutazione di impatto, il Titolare ritenga che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e di costi di attuazione e dovesse risultare dalla valutazione d'impatto che il trattamento (in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio) possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, dovrà ricorrere alla **consultazione preventiva dell'Autorità** ai sensi dell'art. 36 RGPD.

13.1 Flow Chart Valutazione d'impatto



14. Formazione

Per un efficace funzionamento del Modello, la formazione degli Autorizzati e dei Data Manager, ove nominati, è gestita dalla Società in stretta cooperazione con il Privacy Officer.

In particolare, i corsi di formazione hanno ad oggetto l'intero Modello in tutte le sue componenti nonché le nozioni relative alle Leggi sulla protezione dei dati applicabili.

La partecipazione ai corsi di formazione è monitorata attraverso un sistema di rilevazione delle presenze.

Al termine di ogni corso di formazione è sottoposto al partecipante un test finalizzato a valutare il grado di apprendimento conseguito ed ad orientare ulteriori interventi formativi.

La partecipazione ai corsi di formazione è obbligatoria per tutto il personale in servizio presso la Società. Tale obbligo costituisce una regola fondamentale del presente Modello, alla cui violazione sono connesse le sanzioni previste nel sistema disciplinare.

I destinatari della formazione, sono tenuti a:

- acquisire conoscenza dei principi e dei contenuti del Modello;
- conoscere le modalità operative con le quali deve essere realizzata la propria attività;
- contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.

15. Inosservanza del Modello Organizzativo

Si porta a conoscenza di tutti i Destinatari che il presente Modello Organizzativo, nonché le Procedure e policy che ne formano parte integrante, ha carattere vincolante per i Destinatari.

Eventuali violazioni del presente Modello e delle Procedure che formano parte integrante e sostanziale del Modello, da intendersi integralmente richiamate e trascritte, possono avere gravi ripercussioni sulla Società e comportare, nei confronti del dipendente inadempiente, l'applicazione di provvedimenti disciplinari, in conformità alle disposizioni di legge e del CCNL applicabile e nei confronti degli altri Destinatari anche la cessazione del rapporto contrattuale.

I comportamenti che costituiscono violazione del presente Modello possono determinare, nel contempo, la violazione di disposizioni di legge tali da implicare per l'utilizzatore inadempiente conseguenze di natura civile e penale.

Anche la Società può essere perseguita e sanzionata in conseguenza della condotta dei Destinatari. Agli stessi potrà dunque venire richiesto di risarcire i danni derivati dalle violazioni della presente Procedura.

16. Contatti

In caso di quesiti o dubbi in merito all'applicazione del presente Modello Organizzativo e/o in merito a qualsivoglia Procedura, si prega di contattare:

- Privacy Officer
  - E-mail: privacybkri@burgerking.it
  - Tel.: 3351930709

- Responsabile IT:
  - E-mail: carmine.torella@burgerking.it
  - Tel.: 3482708154

ALLEGATO 1

PROCEDURA SULLA CONSERVAZIONE DEI DATI PERSONALI

Data Retention Policy

[OMISSIS]

ALLEGATO 2

DATA BREACH POLICY

1. INTRODUZIONE

Il RGPD introduce in capo agli enti che pongono in essere attività di trattamento di Dati personali, l'obbligo di notificare all'Autorità eventuali violazione dei Dati personali trattati, a meno che il Titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora da tale violazione derivino rischi elevati per le persone fisiche, l'obbligo di comunicazione si estende anche ai singoli Interessati coinvolti.

In ragione delle attività di trattamento di Dati personali svolte, Burger King Restaurants Italia S.r.l. ha ritenuto necessario adottare la presente Data Breach Policy al fine di disciplinare le opportune modalità di gestione del Data Breach, individuando le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di trattamento di Dati personali di cui Burger King Restaurants Italia S.r.l. è Titolare del trattamento.

2. OBBLIGAZIONI GENERALI

In ragione degli obblighi gravanti sul Titolare, i Destinatari sono tenuti a rispettare la presente procedura (i.e. *Data Breach Policy*). In particolare:

- i dipendenti e collaboratori della Società, nello svolgimento delle attività di propria competenza, sono responsabili della comunicazione tempestiva di potenziali o attuali violazioni dei Dati personali al proprio al Privacy Officer, nonché di prestare la massima collaborazione nello svolgimento delle attività di verifica e di contenimento delle violazioni in essere;
- i Responsabili del trattamento dei dati ed ogni altro soggetto terzo che effettua operazioni di trattamento dei dati di cui la Società è Titolare sono tenuti a comunicare tempestivamente al Titolare potenziali violazioni dei Dati personali e fornire tutta l'assistenza necessaria affinché il Titolare adempia alle obbligazioni previste dalle Leggi sulla protezione dei dati;
- Il Privacy Officer quale punto di riferimento all'intero della Società per la corretta applicazione e diffusione delle disposizioni previste dalle Leggi sulla protezione dei dati, è tenuto a verificare costantemente la corretta applicazione delle norme di condotta definite

dalla presente procedura, condurre le attività di indagine necessarie ad accertare l'eventuale Data Breach, assistere il Titolare ad effettuare le segnalazioni all'Autorità e/o le comunicazioni agli Interessati nonché a manutenere il registro delle violazioni segnalate.

3. NORME DI COMPORTAMENTO IN CASO DI DATA BREACH

3.1 Norme di comportamento per i Destinatari

In caso di violazione di sicurezza che, anche solo potenzialmente, possa apparire idonea a generare un Data Breach, quanto accaduto dovrà **essere immediatamente segnalato comunque non oltre 12 ore** dalla conoscenza della violazione da parte del Destinatario ai punti di contatto indicati al paragrafo 8 che segue.

Al fine di coadiuvare il Privacy Officer nella gestione tempestiva delle attività di notifica della violazione dei Dati personali all'Autorità, il Destinatario dovrà primariamente effettuare la segnalazione tramite e-mail contenente l'indicazione degli elementi fondamentali della possibile violazione, con ciò intendendosi:

- una breve descrizione della natura della violazione;
- l'indicazione di categorie e numero approssimativo di dati coinvolti;
- l'indicazione di categorie e numero approssimativo di Interessati coinvolti;
- l'indicazione delle misure adottate per la limitazione delle conseguenze derivanti dalla violazione in essere.

Tale attività potrà essere svolta compilando l'apposito form di cui al paragrafo 5 che segue.

Nell'immediatezza dell'evento, il Destinatario dovrà adottatore ogni misura idonea a bloccare o, in ogni caso, a limitare le conseguenze derivanti dalla violazione dei Dati personali in essere.

Ti ricordiamo che, in caso di Data Breach, la Società ha l'obbligo, entro 72 ore dal momento in cui ne è venuta a conoscenza, di notificare all'Autorità la violazione. Pertanto, in caso di violazioni di sicurezza anche solo potenziali, ti invitiamo a segnalare l'accaduto ai punti di contatto di cui al Paragrafo 5.

3.2 Analisi preliminare ed elaborazione della Scheda evento

Qualora venga segnalata una possibile violazione dei Dati personali, il Privacy Officer, in collaborazione con il Responsabile IT, deve svolgere le necessarie indagini ed avviare un'analisi preliminare provvedendo a compilare la Scheda Evento di cui al paragrafo 6 che segue.

Il Privacy Officer, in collaborazione con il Responsabile IT, è tenuto a comunicare immediatamente al Titolare le risultanze delle anzidette indagini al fine di consentire allo stesso di qualificare correttamente la violazione di sicurezza e valutare la necessità o meno di effettuare la notificazione all'Autorità.

Nel caso in cui la segnalazione effettuata dal Destinatario **risulti infondata**, il Privacy Officer provvede ad archiviare l'incidente. In ogni caso, il Privacy Officer è tenuto a dare evidenza del c.d. falso positivo all'interno del Registro dei Data Breach, di cui al paragrafo 7 che segue, nella apposita sezione dedicata agli "incidenti infondati".

Nel caso in cui la segnalazione **non** risulti infondata, il Privacy Officer verifica se la violazione possa comportare un rischio per i diritti e le libertà delle persone fisiche.

3.3 Norme di condotta per il Privacy Officer

3.3.1 Notifica all'Autorità

Nel caso in cui la violazione di sicurezza **non** si dimostri idonea a rappresentare un rischio elevato per i diritti e le libertà del degli Interessati coinvolti, il Privacy Officer procede, per conto del Titolare, alla registrazione della violazione e all'archiviazione di quanto segnalato avvalendosi del registro di cui al paragrafo 7 che segue.

Qualora la violazione **possa comportare un rischio per i diritti e le libertà delle persone fisiche**, il Titolare, assistito dal Privacy Officer, provvede ad effettuare la notifica all'Autorità nel limite delle 72 ore successive al momento in cui si è avuta consapevolezza dell'avvenuta violazione, nonché alla comunicazione agli Interessati coinvolti secondo le disposizioni di cui al paragrafo 3.3.2 che segue.

La notifica all'Autorità deve almeno:

a) **descrivere la natura della violazione** dei Dati personali compresi, ove possibile, le categorie e il numero approssimativo di Interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei Dati personali in questione;
b) **comunicare il nome e i dati di contatto del RPD o di altro punto di contatto** presso cui ottenere più informazioni;
c) **descrivere le probabili conseguenze** della violazione dei Dati personali;

d) **descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento** per porre rimedio alla violazione dei Dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le anzidette informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Privacy Officer dovrà in ogni caso **documentare le violazioni** di Dati personali subite, anche se non notificate all'Autorità e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati

3.3.2 Comunicazione agli Interessati

Nel caso in cui il Data Breach presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Privacy Officer e/o il Data Manager, ove nominato, deve assistere il Titolare del trattamento affinché lo stesso comunichi la violazione agli Interessati senza ingiustificato ritardo.

La comunicazione agli Interessati deve avvenire mediante il canale di volta in volta ritenuto più idoneo e deve essere effettuata con un linguaggio semplice e chiaro.

La comunicazione agli Interessati deve contenere almeno le seguenti informazioni:

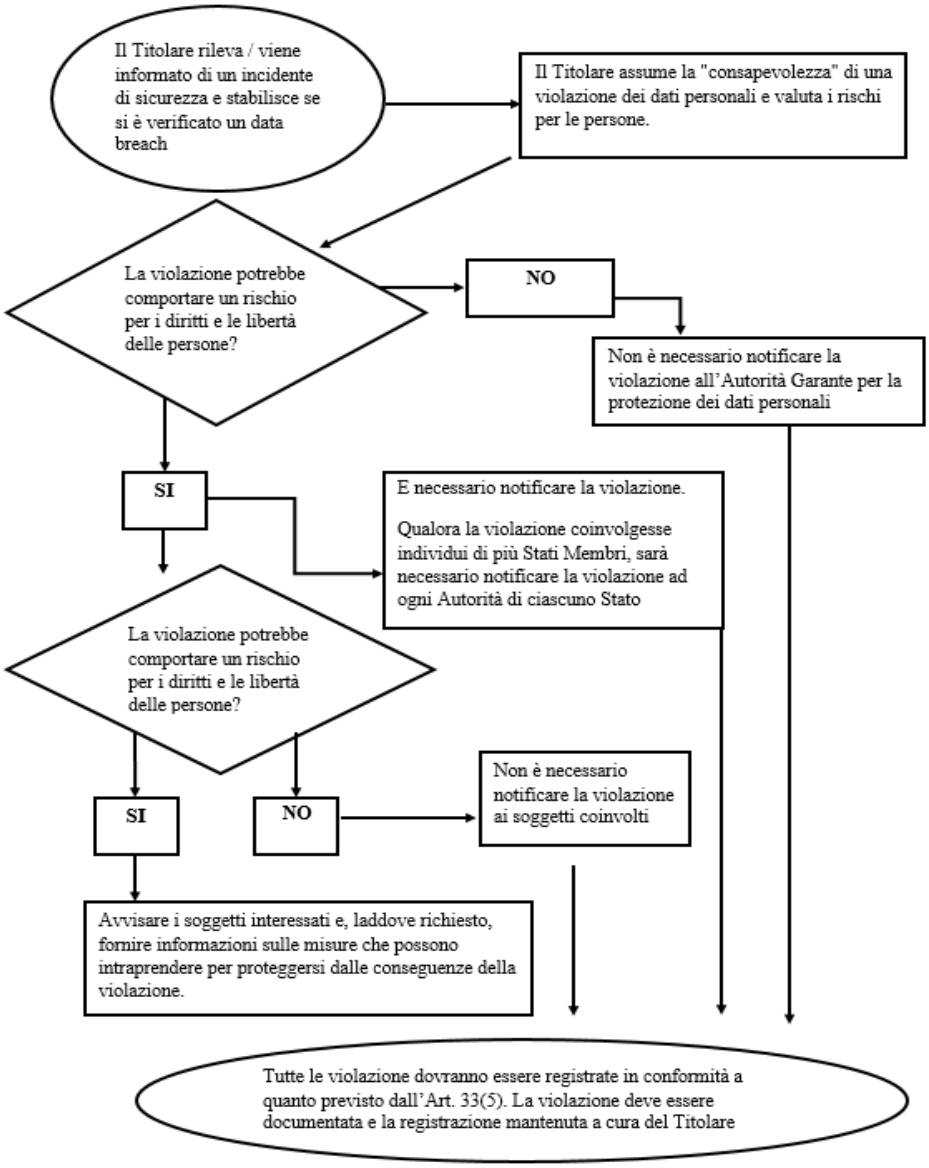
a) La natura della violazione;
b) Il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
c) La descrizione delle probabili conseguenze della violazione dei Dati personali;
d) La descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione e anche, se del caso, per attenuare i possibili effetti negativi.

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati personali oggetto della violazione, in particolare quelle destinate a rendere i Dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

Anche in caso di notificazione all'Autorità e/o agli interessati il Privacy Officer procede, per conto del Titolare, alla registrazione della violazione avvalendosi del registro di cui al paragrafo 7 che segue.

4. FLOW CHART DATA BREACH POLICY



5. FORM PER LA SEGNALAZIONE DI VIOLAZIONI DI SICUREZZA

Informazione richiesta		*Risposta*
Dati identificativi del segnalante		
Descrizione della violazione		
Ora e data di identificazione della violazione		
Indicazione del trattamento inerente il dato violato (anche se non censito nel Registro dei trattamenti)		
Banca dati o archivi anche cartacei che sono stati violati:		
Tipo di violazione:		**Lettura** *(presumibilmente i dati non sono stati copiati)*
		Copia *(i dati sono ancora presenti nel sistema del Titolare)*
		Modifica *(i dati sono presenti nei sistemi ma sono stati irreversibilmente modificati, senza possibilità di ripristino)*
		Distruzione *(i dati non sono nella disponibilità del Titolare né di altri)*
		Furto *(i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)*
		Altro:
Dispositivo oggetto della violazione:		**Computer**
		Rete
		Dispositivo mobile
		File o parte di un file
		Strumento di back up
		Documento cartaceo
		Altro: _____
Tipologia di Dati personali oggetto di violazione		**Dati anagrafici / codice fiscale**
		Dati di accesso e di identificazione *(username, password, customer ID, etc.)*
		Dati relativi a minori
		Particolari categorie di dati *(origine razionale ed etnica, convinzioni religiose, filosofiche, opinioni politiche, adesione a sindacati etc.)*
		Dati economico – finanziari *(es. numero carta di credito)*
		Dati genetici
		Dati relativi alla salute

		Dati giudiziari
		Dati biometrici
		Altro: _____
Categorie di soggetti coinvolti		**Candidati**
		Dipendenti
		Utenti
		Fornitori
		Clienti
		Agenti
		Consulenti
		Amministratori della Società
		Sindaci della Società
		Altro: _____
Numero di interessati coinvolti nella violazione		**N. ___ persone (sia certo sia approssimativo)**
		Numero (ancora) sconosciuto
Volume di dati coinvolti nella violazione		
Stato della violazione (attuale o limitata)		
Breve descrizione delle misure adottate per limitare le conseguenze		
Dati di contatto del segnalante (Telefono, e-mail)		
Ulteriori persone informate della violazione		
Ogni altra informazione rilevante		

6. SCHEDA EVENTO

Istruzioni per la valutazione del livello di rischio:

Il livello di rischio derivante da una violazione di Dati personali deve tenere conto della probabilità che si verifichi a danno delle persone fisiche (anche diverse dall'Interesse a cui ineriscono i Dati personali oggetto di violazione) una delle seguenti condizioni:

- Discriminazione
- Perdite finanziarie
- Furto di identità
- Pregiudizio alla segretezza di Dati personali protetti da segreto professionale
- Danno economico o sociale significativo
- Danni fisici, materiali o immateriali alle persone fisiche

Al fine di determinare il livello di rischio associato ad una violazione di Dati personali è altresì necessario tenere in considerazione i seguenti elementi:

- la violazione ha riguardato particolari categorie di Dati personali,
- gli Interessati sono persone fisiche vulnerabili, in particolare minori,
- la violazione ha riguardato una considerevole quantità di Dati personali;
- la violazione ha riguardato un considerevole numero di Interessati.

Data evento e ora della violazione anche solo presunta (specificando se è presunta)	
Data e ora in cui si è avuto conoscenza della violazione	
Fonte della segnalazione	
Tipologia evento	
Descrizione dell'evento	
Numero Interessati coinvolti	
Consistenza quantitativa e qualitativa dei Dati personali presumibilmente coinvolti nella violazione	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito dello	

smarrimento di dispositivi mobili o supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti (indicare anche la loro ubicazione)	

Livello di rischio:

- ☐ NULLO
- ☐ BASSO
- ☐ MEDIO
- ☐ ALTO

7. REGISTRO DEI DATA BREACH

EVENTO			CONSEGUENZE	PROVVEDIMENTI ADOTTATI	NOTIFICA ALL'AUTORITA'		COMUNICAZIONE ALL'INTERESSATO		Firma del Titolare
Data Violazione	***Tipologia violazione*** *(si prega di indicare:* *- il sistema impattato dalla violazione* *- categorie di dati coinvolti* *- categorie di Interessati cui appartengono i dati della violazione)*	***Incidente infondato***			***SI/NO***	***Data***	***SI/NO***	***Data***	

8. CONTATTI

In caso di possibile violazione di Dati personali, si prega di contattare:

- Privacy Officer
  - E-mail: privacybkri@burgerking.it
  - Tel.: 3351930709

- Responsabile IT:
  - E-mail: carmine.torella@burgerking.it
  - Tel.: 3482708154

ALLEGATO 3

PROCEDURA PER L'ESERCIZIO DEI DIRITTI DEGLI INTERESSATI

1. INTRODUZIONE

Il RGPD pone particolare attenzione alla tutela dei diritti degli Interessati i cui Dati personali sono oggetto di Trattamento.

In ragione delle operazioni di Trattamento di Dati personali effettuate, la Società ha ritenuto necessario adottare la presente procedura al fine di indicare ai Destinatari le azioni da compiere per garantire agli Interessati l'agevole esercizio dei diritti riconosciuti dal RGPD.

In particolare, il RGPD consente agli Interessati di richiedere al Titolare del Trattamento di:

- accedere ai propri dati e ricevere informazioni relative ai trattamenti effettuati dal Titolare (Art. 15 RGPD);
- ottenere la rettifica dei Dati personali inesatti che lo riguardano (Art. 16 RGPD);
- richiedere la cancellazione dei propri dati (Art. 17 RGPD);
- ottenere, ove consentito, la limitazione del trattamento (Art. 18 RGPD);
- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano (Art. 20 RGPD);
- opporsi in qualsiasi momento al trattamento dei Dati personali che lo riguardano (Art. 21 RGPD);
- non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla persona (Art. 22 RGPD).

Da ultimo si fa presente che il RGPD conferisce agli Interessati il diritto di proporre reclamo all'Autorità ai sensi dell'art. 77 RGPD nel caso in cui l'interessato ritenga che il Trattamento violi il RGPD.

2. SCOPO E AMBITO DI APPLICAZIONE

Lo scopo della presente Procedura per l'esercizio dei diritti degli Interessati è quello di disciplinare le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di Trattamento di Dati personali di cui la Società è Titolare al fine di agevolare e garantire l'esercizio dei Diritti degli Interessati.

In conformità con quanto previsto dalle disposizioni del RGPD, anche il Responsabile del trattamento dei dati sarà tenuto a collaborare con il Titolare ai fini del proficuo esercizio dei diritti

degli Interessati. A tale ultimo riguardo, il Titolare ha provveduto a nominare, mediante apposito accordo scritto, i soggetti che trattano dati in nome e per conto del Titolare in qualità di Responsabili del Trattamento. Tali soggetti si sono impegnati a fornire al Titolare l'assistenza necessaria al fine di garantire il corretto esercizio dei diritti degli Interessati.

Le norme di condotta descritte in questa procedura si applicheranno a tutte le informazioni relative a Dati personali oggetto di trattamento da parte del Titolare. Gli Interessati coinvolti potranno essere a titolo indicativo e non esaustivo:

- Clienti;
- Ex clienti;
- Potenziali clienti;
- Dipenditi;
- Ex dipendenti;
- Candidati;
- Fornitori e Consulenti.

3. DIRITTI DEGLI INTERESSATI

Il RGPD fornisce agli Interessati determinati diritti previsti dagli artt. 15-22. Sarà, pertanto, necessario da parte dei Destinatari della presente procedura assistere il Titolare affinché possa garantire agli Interessati l'esercizio dei seguenti diritti:

- **Diritto di accesso:** l'Interessato ha il diritto di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di Dati personali che lo riguardano e, in tal caso, ottenere l'accesso ai Dati personali e alle seguenti informazioni:
  - le finalità del trattamento;
  - le categorie di Dati personali trattati;
  - i destinatari o le categorie di destinatari a cui i Dati personali sono stati o saranno comunicati;
  - ove possibile, il periodo di conservazione dei Dati personali ovvero, se non è possibile i criteri utilizzati per determinare tale periodo;
  - l'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei Dati personali che lo riguardano o di opporsi al loro trattamento;
  - il diritto di proporre reclamo all'Autorità;

- qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.

- **Diritto di rettifica:** l'Interessato ha il diritto di ottenere dal Titolare, senza ingiustificato ritardo, la rettifica dei Dati personali inesatti che lo riguardano. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei Dati personali incompleti, anche fornendo una dichiarazione integrativa.
- **Diritto alla cancellazione:** l'Interessato ha il diritto di ottenere, al ricorrere degli specifici presupposti richiesti dalle Leggi sulla protezione dei dati applicabili, dal Titolare la cancellazione dei Dati personali che lo riguardano senza ingiustificato ritardo se sussiste uno dei seguenti motivi:
  - i Dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
  - l'Interessato revoca il consenso su cui si basa il trattamento e non vi sono ulteriori basi giuridiche che legittimino il trattamento;
  - l'Interessato si oppone al Trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
  - i Dati personali sono stati trattati illecitamente;
  - i Dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare;
- **Diritto di limitazione di trattamento:** l'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento effettuato in presenza di una delle seguenti condizioni:
  - l'Interessato contesta l'esattezza dei Dati personali. In tal caso, per il periodo necessario al Titolare del trattamento a verificare l'esattezza di tali Dati personali, l'Interessato potrà richiedere la limitazione del trattamento dei propri dati;
  - il trattamento è illecito e l'Interessato si oppone alla cancellazione dei Dati personali e chiede, invece, che ne sia limitato l'utilizzo;
  - i Dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

- l'Interessato si è opposto al trattamento; in tal caso ha diritto di richiedere la limitazione del trattamento in attesa della verifica da parte del Titolare in merito all'eventuale prevalenza dei motivi legittimi di quest'ultimo rispetto a quelli dell'Interessato.

- **Diritto alla portabilità dei dati:** l'Interessato ha il diritto di ricevere dal Titolare i Dati personali che lo riguardano forniti al Titolare in un formato strutturato, di uso comune e leggibile da dispositivo automatico e ha il diritto di trasmettere tali Dati personali a un altro titolare qualora:
  - il trattamento dei propri dati sia effettuato da parte del Titolare sulla base del consenso e/o sia necessario all'esecuzione di un contratto; **e**
  - il trattamento sia effettuato con mezzi automatizzati.
- **Diritto di opposizione:** l'Interessato ha il diritto di opporsi in ogni momento, per ragioni connesse alla sua particolare situazione, al trattamento dei Dati personali che lo riguardano. Tale richiesta può essere esercitata qualora il trattamento sia effettuato da parte del Titolare sulla base di un legittimo interesse dello stesso e/o qualora il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico. In tal caso il Titolare del trattamento si astiene dal trattare ulteriormente i Dati personali salvo che lo stesso dimostri l'esistenza di motivi legittimi cogenti prevalenti sugli interessi e/o diritti dell'Interessato.

  Qualora i Dati personali siano trattati per **finalità di marketing diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei Dati personali che lo riguardano effettuato per tali finalità compresa la profilazione nella misura in cui sia connessa alle attività di marketing diretto**.

4. PROCEDURA PER L'INVIO DI UNA RICHIESTA

4.1. Privacy Officer

Il Titolare ha creato un apposito indirizzo mail privacybkri@burgerking.it per consentire agli Interessati di poter esercitare agevolmente i diritti riconosciuti dal RGPD. La gestione di tale indirizzo mail è affidata al Privacy Officer il quale ha il compito, tra l'altro, di consultare periodicamente la casella di posta dedicata alla gestione delle richieste presentate dagli Interessati al Titolare.

Al momento del ricevimento della richiesta da parte dell'Interessato il Privacy Officer ha il compito di inviare tempestivamente una mail all'Interessato informandolo del fatto che la richiesta presentata è in corso di elaborazione da parte del Titolare. Il Privacy Officer, contestualmente, richiederà all'Interessato di compilare il format di cui al paragrafo 8 che segue.

Qualora non fosse possibile per l'Interessato inviare la richiesta via e-mail, il modulo potrà essere inviato via posta ordinaria tramite raccomandata a.r. presso la sede della Società all'indirizzo: Burger King Restaurants Italia S.r.l., Strada 1, Palazzo F4, Assago Milanofiori (MI).

Sarà inoltre compito del Privacy Officer individuare il Data Manager, ove nominato, e/o l'Autorizzato che nello specifico caso può essere coinvolto per evadere la richiesta presentata dall'Interessato.

Esempi

In caso di richiesta ricevuta da dipendenti il Privacy Officer representative coinvolgerà il Responsabile HR.

In caso di richieste ricevuta da clienti il Privacy Officer representative coinvolgerà il Responsabile Marketing etc.)

Il Privacy Officer è, altresì, incaricato del mantenimento del registro delle richieste presentate dagli Interessati al Titolare di cui al paragrafo 9 che segue.

4.2. Data Manager e Responsabili del trattamento dei dati

Al momento del ricevimento della richiesta di supporto da parte del Privacy Officer, il Data Manager, ove nominato, e/o l'Autorizzato avrà il compito di fornire tutta l'assistenza necessaria affinché il Privacy Officer secondo le tempistiche di cui al **paragrafo 6** che segue, possa dare riscontro alla richiesta presentata dall'Interessato.

Sarà inoltre compito del Data Manager di riferimento, ove nominato, e/o dell'Autorizzato interfacciarsi con eventuali Responsabili esterni del trattamento e/o altre società del gruppo di cui il Titolare si avvale per le operazioni di trattamento dati che riguardano l'Interessato.

Esempi

In caso di richiesta ricevuta da dipendenti, il Responsabile HR, nella sua qualità di Data Manager, coinvolgerà, se necessario, la Società che eroga i servizi di payroll.

In caso di richiesta ricevuta da clienti il Responsabile Marketing, nella sua qualità di Data Manager, coinvolgerà, se necessario, la Società che gestisce il sito web e/o la App dela Società.

Il Responsabile del trattamento dei dati ha il compito di fornire al Data Manager di riferimento, ove nominato, e/o all'Autorizzato tutto il supporto necessario per gestire la richiesta presentata dall'Interessato.

5. LIMITAZIONI

Il Privacy Officer, previa valutazione congiunta con il Titolare del Trattamento, potrà rifiutare di soddisfare la richiesta formulata da parte dell'Interessato nel caso in cui questa si riveli manifestamente infondata o eccessiva, in particolare per il carattere ripetitivo della stessa.

Il Privacy Officer, previa valutazione congiunta con il Titolare del Trattamento, può altresì rifiutare, limitare o differire le informazioni, nella misura concessa dalla legge o quando sia necessario per proteggere interessi sovrastanti di terzi o del Titolare del trattamento. In tal caso, il Titolare del trattamento deve provare l'interesse legittimo e bilanciarlo con gli interessi dell'Interessato richiedente le informazioni. Il Titolare può limitare le informazioni solo se i suoi interessi o quelli di terzi prevalgono su quelli dell'Interessato.

6. TEMPISTICHE

In ogni caso, il Privacy Officer, farà pervenire all'Interessato le informazioni oggetto della richiesta senza ingiustificato ritardo e comunque, al più tardi, **entro un mese** dal *ricevimento* della richiesta stessa. Tale termine, tenuto conto della complessità e del numero delle richieste, può essere prorogato, se necessario, di **due mesi**.

In caso di impossibilità di fornire le informazioni entro il **termine di un mese**, il Privacy Officer, con il supporto del Data Manager e/o Responsabile del trattamento dei dati ha il compito di avvertire l'Interessato **entro un mese dal ricevimento della richiesta**.

7. COSTI

La fornitura delle informazioni è gratuita e, ove possibile e salvo richiesta diversa dell'Interessato, avviene tramite mezzi elettronici.

In via eccezionale, il Titolare del trattamento potrebbe porre a carico dell'Interessato un contributo spese qualora:

a) la richiesta dell'Interessato sia manifestamente infondata o eccessiva;
b) l'Interessato richieda la realizzazione di copie ulteriori da parte del Titolare del trattamento.

In particolare, la sopra indicata ipotesi sub *a)* si potrebbe verificare qualora il richiedente abbia già ricevuto le informazioni richieste e non possa provare alcun interesse legittimo, idoneo a giustificare un'ulteriore fornitura delle informazioni, oppure in caso di richieste frequenti.

La sopra indicata ipotesi sub *b)* inerisce all'addebito di spese per le sole copie successive alla prima su supporto fisico, e non anche alle copie elettroniche prive di supporto, in quanto queste ultime sono replicabili senza che il Titolare del trattamento debba sostenere costi ulteriori.

8.MODULO DI RICHIESTA DI ACCESSO AI DATI DELL'INTERESSATO

Si prega di compilare il presente modulo e inviarlo, **unitamente alla copia di un documento d'identità in corso di validità**, al **Titolare** al seguente indirizzo email: privacybkri@burgerking.it ovvero tramite l'invio di raccomandata a.r. presso la sede della Società all'indirizzo: Burger King Restaurants Italia S.r.l., Strada 1, Palazzo F4, Assago Milanofiori (MI).

Le informazioni fornite in relazione a questa richiesta verranno trattate al solo scopo di elaborare e rispondere alla richiesta e successivamente eliminate salvo il diritto del Titolare di adempiere ad obblighi legali a cui è soggetto e tutelare i propri interessi in sede di giudizio.

È necessario che Lei provveda a compilare tutti i campi sottostanti al fine di consentire una corretta elaborazione della Sua richiesta da parte del Titolare. In caso di Sua non integrale compilazione del presente modulo, potremmo contattarla per ottenere le informazioni mancanti e, in tal caso, l'elaborazione della Sua richiesta potrebbe essere posticipata fino a quando non fornirà le informazioni necessarie.

1. Dati del Richiedente

Nome e Cognome	
Indirizzo	
Codice postale / Città	
Numero di telefono	
Indirizzo e-mail	

2. Dati dell'Interessato (se diverso dal Richiedente)

Nome e Cognome	
Indirizzo	
Codice postale / Città	
Numero di telefono	
Indirizzo e-mail	

3. Rapporti con Burger King Restaurants Italia S.r.l.

	Cliente
	Ex Cliente
	Potenziale Cliente
	Dipendente
	Ex Dipendente
	Fornitore
	Consulente
	Altro (Specificare)

4. Quali diritti intende esercitare?

	Diritto di accesso
	Diritto di rettifica
	Diritto alla cancellazione
	Diritto di limitazione di trattamento
	Diritto alla portabilità dei dati
	Diritto di opposizione
	Diritto di accesso
	Diritto di rettifica

5. Descrizione della richiesta

Si prega di indicare nel seguito il contenuto della richiesta che Lei intende avanzare nei confronti del **Titolare**. Si raccomanda di essere quanto più specifici possibile per consentire al **Titolare** di dare tempestivo riscontro fornendo informazioni accurate e complete.

_____

_____

_____

_____

Se il Richiedente non è l'Interessato, si prega di allegare una delega o altro strumento equivalente che fornisca prova che il Richiedente è legittimato a richiedere informazioni sull'Interessato.

Data: _____

Firma: _____.

9. REGISTRO DELLE RICHIESTE PRESENTATE DAGLI INTERESSATI

Data Richiesta	Riferimenti Richiedente e categoria di appartenenza *(e.g. cliente, dipendente etc.)*	Tipo di richiesta *(e.g. richiesta di accesso, cancellazione, opposizione ecc.)*	Funzioni coinvolte	Azione intrapresa *(e.g. cancellazione dei dati dal CRM per finalità di Marketing, aggiornamento dei dati etc.)*	Data di chiusura della richiesta