Modello Organizzativo Privacy

Titolo	Modello Organizzativo Privacy
Data	11/10/2023
Versione	2.0

INDICE

1. Finalità

Il Regolamento in materia di protezione dei dati personali (UE) n. 2016/679 (nel seguito, "**GDPR"**) 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 e l'art. 5, par.2 GDPR prevedono che il Titolare del trattamento metta in atto misure tecniche ed organizzative adeguate ed efficaci al fine di garantire, ed essere in grado di dimostrare, che il trattamento dei Dati personali abbia luogo in conformità alle Leggi sulla protezione dei dati applicabili.

A tal fine, la società **Burger King Restaurants Italia S.p.A.** con sede legale in Assago (MI), 20057 - strada 1, Palazzo F4-F5 Milanofiori, P.IVA e C.F. 08876390967 (di seguito, la "**Società**" o il "**Titolare**") ha ritenuto necessario adottare il presente Modello Organizzativo Privacy (nel seguito, anche il "**Modello Privacy**" o il "**Modello**") al fine di specificare i presidi organizzativi e di processo di cui si 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 Privacy 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 Privacy, 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:

Amministratori di sistema	indica le figure professionali nominate ai sensi del Provvedimento *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"*.
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.
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 ai sensi dell'art. 29 GDPR e dell'art. 2 quaterdecies del D.lgs. 196/2003.
Codice di Condotta	indica il Codice di Condotta in materia di protezione dei dati personali adottato dalla Società e parte integrante e sostanziale del presente Modello Privacy.
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.
Categorie Particolari di dati personali	indica, ai sensi dell'art. 9 GDPR, i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
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 Giudiziari	indica i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
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.
Data Protection Officer o DPO	indica – ove designato ai sensi dell'art. 37 GDPR – il Responsabile della Protezione dei Dati, un soggetto che sovrintende alla conformità della protezione dei dati di un'organizzazione.
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, se del caso, le Procedure.
Informativa	indica le informative ai sensi degli artt. 13 e 14 del GDPR che il Titolare rende di volta in volta in favore degli interessati.
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 (GDPR) 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 adottato dalla Società al fine di garantire la corretta gestione e implementazione dei presidi previsti dalle Leggi sulla protezione dei dati.
Paese terzo	indica un paese al di fuori dello Spazio Economico Europeo.
Privacy Responsible	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 ed ogni eventuale ulteriore procedura adottata dalla Società in materia di protezione dei dati personali.
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 la Società 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 GDPR, 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 incaricata dalla Società ai sensi dell'art. 28 del GDPR a trattare Dati personali per conto del Titolare del trattamento dei dati.
GDPR	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, ai fini del presente Modello, Burger King Restaurants Italia S.p.A. con sede legale in Assago (MI), 20057 – strada 1, Palazzo F4 Milanofiori, P.IVA e C.F. 08876390967.
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.

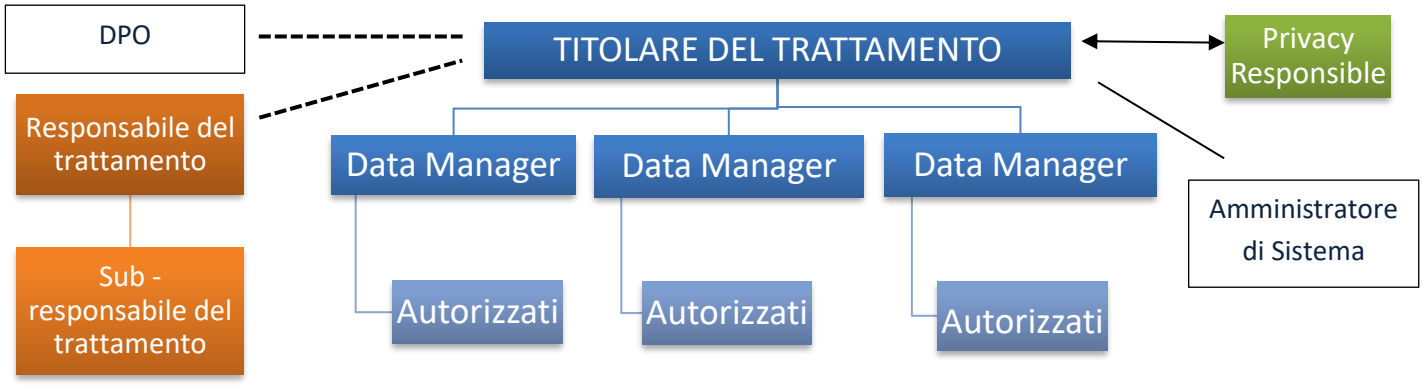
4. Ruoli e responsabilità

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. Al Titolare del trattamento spetta il compito di definire e 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 GDPR;
  - consultare l'Autorità nei casi e secondo le modalità previste dall'Art. 36 GDPR;
  - nominare i Responsabili del trattamento ai sensi dell'art. 28 del GDPR;
  - nominare gli Autorizzati ai sensi dell'art. 29 del GDPR e dell'art. 2 quaterdecies del Codice Privacy.
- **Il DPO** è il soggetto che è chiamato a svolgere le attività di cui all'art. 39 del GDPR. Nell'espletamento delle sue funzioni, il DPO deve assistere il Titolare e il Privacy Responsible nell'attuazione delle Procedure, fungendo altresì da punto di contatto per gli Interessati e per l'Autorità di controllo.
- **Il Privacy Responsible** è il soggetto che è chiamato a supervisionare e a sovrintendere l'effettiva implementazione del Modello Organizzativo Privacy.
- **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.
- **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 GDPR.

- **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.
- **Gli Amministratori di sistema** sono i soggetti, nominati ai sensi del Provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008", incaricati della gestione e della manutenzione di un impianto di elaborazione o di sue componenti, ivi comprese le basi dati e l'infrastruttura di rete.

4.1 Flow Chart Data Protection Governance



5. Principi e Liceità del trattamento

L'art. 5 del GDPR stabilisce alcuni principi[1] applicabili al trattamento dei dati personali che i Destinatari sono chiamati a rispettare nello svolgimento delle operazioni di trattamento. Sul punto, il Titolare ha adottato uno specifico Codice di Condotta.

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

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;

[1] Art. 5 del GDPR: "*I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).*"

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 DPO e/o al Privacy Responsible e/o al Data Manager di riferimento.

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.
A tal riguardo i Destinatari sono tenuti a raccogliere il consenso da parte degli Interessati e provvedere alla relativa conservazione dello stesso. Gli Autorizzati sono, inoltre, tenuti ad assistere il Privacy Responsible e, se del caso, il DPO affinché il Titolare 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 all'avvio del trattamento** un **test comparativo** atto a verificare la liceità del Trattamento medesimo. Tale test comparativo si articola nelle seguenti fasi:

a) **Purpose Test:** è necessario, in primo luogo, identificare l'interesse che il Titolare del trattamento intende perseguire. Sul punto, quindi, il Privacy Responsible, se del caso con il supporto del DPO, deve valutare se l'interesse perseguito sia sufficientemente concreto e/o reale, e non meramente teorico. In tale contesto, si rende necessario valutare altresì se l'interesse perseguito e come identificato sia "legittimo" ossia perseguibile secondo modalità conformi alle Leggi sulla protezione dei dati.

b) **Necessity Test:** è necessario, in secondo luogo, che il Privacy Responsible 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 derivanti da tale tipologia di trattamento sui diritti e/o gli interessi fondamentali dell'Interessato;
- Le ragionevoli aspettative dell'Interessato anche sulla base della relazione intrattenuta da quest'ultimo con il Titolare;
- 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 – previo parere del DPO – potrà avviare il trattamento, avendo cura di informare gli interessati 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 Privacy Responsible è tenuto a documentare per iscritto il test comparativo, avendo cura di archiviare la documentazione inerente al bilanciamento effettuato e ai relativi esiti. Il Privacy Responsible è

tenuto a conservare, sotto la sua responsabilità, tutta la documentazione inerente, conseguente ed accessoria al test comparativo.

5.3 Il Trattamento di Categorie particolari di dati personali

L'art. 9, par. 1 GDPR prevede un divieto di carattere generale di Trattare le c.d. Categorie particolari di dati personali, salvo che ricorra una specifica condizione di liceità del trattamento (prevista ai sensi dell'art. 9, par. 2 GDPR) corrispondente ad altrettanti prevalenti interessi ritenuti meritevoli di tutela dall'ordinamento.
Sul punto, si precisa infatti che "*meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali*"[2].
Pertanto, ai sensi dell'art. 9 GDPR, il Trattamento di Categorie particolari di dati può avere luogo solo qualora:

1. L'interessato abbia prestato il proprio **consenso esplicito** al Trattamento di tali Dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1 dell'art. 9 GDPR;
2. il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato **in materia di diritto del lavoro e della sicurezza sociale e protezione sociale**, nella misura in cui il Titolare sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
3. il Trattamento è necessario per **tutelare un interesse vitale dell'interessato** o di un'altra persona fisica qualora l'interessato si trovi **nell'incapacità fisica o giuridica di prestare il proprio consenso**;
4. il Trattamento riguarda Dati personali resi manifestamente pubblici dall'interessato;
5. il Trattamento è necessario per **accertare, esercitare o difendere un diritto** in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
6. il Trattamento è necessario per **motivi di interesse pubblico rilevante** sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
7. il Trattamento è necessario per **finalità di medicina preventiva o di medicina del lavoro**, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità. In tal caso si precisa che tali Dati personali sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione Europea o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione Europea o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti;

[2] Rif. Considerando n. 51 del GDPR.

8. il Trattamento è necessario per **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale.

Con particolare riferimento al Trattamento delle Categorie particolari di dati nell'ambito del rapporto di lavoro, la Società impone il rispetto delle Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016).

A tal riguardo i Destinatari sono tenuti ad accertarsi, prima di porre in essere qualsivoglia operazione di Trattamento di Categorie particolari di dati personali, del fatto che sussiste almeno uno dei requisiti 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 DPO, se del caso, per il tramite del Privacy Responsible.

5.4 Il Trattamento di Dati Giudiziari

Il Trattamento di Dati Giudiziari può essere effettuato esclusivamente nei limiti di cui all'art. 10 del GDPR e dell'art. 2 *octies* del Codice Privacy.

Il Titolare, nel rispetto del principio di limitazione del trattamento e proporzionalità, ove possibile, si astiene dal Trattamento di tali categorie di Dati personali e richiede ai Destinatari, prima di avviare qualsiasi operazione di Trattamento che possa coinvolgere Dati Giudiziari, di rivolgersi al **DPO** affinché possa di volta in volta valutare la liceità del 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 GDPR e le raccomandazioni formulate dal Comitato Europeo per la protezione dei dati[3] 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 DPO;
- 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;

[3] Il comitato europeo per la protezione dei dati è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE.

- 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 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 sua persona;
  - 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.

A tal riguardo i Destinatari sono incaricati della corretta diffusione delle Informative in favore degli interessati. In caso di nuove operazioni di Trattamento gli Autorizzati di riferimento sono tenuti a coinvolgere il DPO e/o il Privacy Responsible anche per il tramite del Data Manager di riferimento 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

Qualora un Trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti delle Leggi sulla protezione dei dati

e garantisca la tutela dei diritti dell'interessato. A tal riguardo, il Privacy Responsible – al momento della selezione e nel corso del rapporto –effettua verifiche finalizzate ad accertare il livello di conformità delle misure tecniche e organizzative adottate dal Responsabile del trattamento ai sensi delle Leggi sulla protezione dei dati mediante l'apposita checklist adottata dal Titolare. L'esito di tali verifiche è soggetto alla valutazione del DPO il quale esprime il proprio parere, richiedendo – se del caso – ulteriori approfondimenti.
In tale contesto, 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 in qualità di Responsabile esterno del trattamento ai sensi dell'art. 28 GDPR.
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 la sede del Titolare.
Per la gestione del Trattamento dei Dati personali effettuato da parte di soggetti terzi per conto del Titolare la Società ha adottato un format di Atto di Nomina.
A tal riguardo i Data Manager e gli Autorizzati ogni qualvolta vi sia la necessità di provvedere alla nomina di soggetti terzi quali Responsabili del trattamento sono tenuti ad assistere il Privacy Responsible al fine di garantire la corretta implementazione di tale presidio.
Il Responsabile del trattamento, a sua volta, è tenuto ad osservare le disposizioni contenute nell'Atto di Nomina sottoscritto con il Titolare nonché le prescrizioni contenute nel Modello Privacy e nel Codice di Condotta.

8. Nomina dell'Amministratore di Sistema

Il Titolare ai sensi del provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" nomina quali Amministratori di sistema i soggetti incaricati della gestione e della manutenzione di un impianto di elaborazione o di sue componenti, ivi comprese le basi dati e l'infrastruttura di rete.
L'attività svolta dagli Amministratori di sistema è sottoposta a verifica annuale formalizzata per il tramite di un'apposita relazione.
Nel caso in cui l'attività di Amministratore di sistema sia svolta da un Responsabile del trattamento e/o da soggetti terzi questi ultimi si impegnano a fornire evidenza dell'adempimento delle misure richieste dal provvedimento di cui sopra.

9. 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 condizioni di cui agli artt. 44 ss. GDPR, ossia:

(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 effettivi. A tal fine, il Privacy Responsible con il supporto del DPO, e dei Data Manager coinvolti è tenuto ad effettuare una valutazione del livello di tutela offerto dal Paese Terzo verso cui si intendono trasferire i Dati personali, c.d. Transfer Impact Assessment.

Possono costituire garanzie adeguate:

- 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 GDPR;
- un meccanismo di certificazione approvato ai sensi dell'art. 42 GDPR.

A tal riguardo i Destinatari sono tenuti ad accertare, 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 DPO, se del caso, per il tramite del Privacy Responsible.

In caso di trasferimenti effettuati da parte del Responsabile del Trattamento, questo è tenuto ad osservare le disposizioni contenute nell'Atto di Nomina sottoscritto con il Titolare nonché le prescrizioni contenute nel Modello Privacy e nel Codice di Condotta.

10. 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 personali 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 DPO e/o il Privacy Responsible per ottenere maggiori informazioni e supporto nello stabilire la legittimità delle finalità, su come documentarla e ottenere, se del caso, 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*), finalizzata 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 GDPR), 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.
Il Responsabile del trattamento è tenuto ad osservare le istruzioni sulle tempistiche di conservazione dei Dati personali impartite dal Titolare e a cancellare/restituire al Titolare i Dati personali secondo le disposizioni contenute nell'Atto di Nomina sottoscritto con il Titolare nonché le prescrizioni contenute nel Modello Privacy e nel Codice di Condotta.

11. 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 oaaetto di trattamento.

Non tutte le violazioni della sicurezza rientrano nella definizione di Data Breach. Affinché si configuri un Data Breach **la violazione deve coinvolgere Dati personali**.
Al fine di garantire una maggiore comprensione, si indicano 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, device elettronici portatili, chiavette USB, smartphone/iPad aziendali;
- ✓ Ransomware;
- ✓ Phishing.

In forza del principio di *accountability,* ossia di responsabilizzazione, il Titolare ha adottato la *Data Breach Policy* ossia una Procedura tesa ad individuare i comportamenti che i Destinatari sono tenuti ad adottare ogniqualvolta si sia verificata 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, inviando tempestivamente un'e-mail al Privacy Responsible all'indirizzo legal@burgerking.it. Il Privacy Responsible, a sua volta, provvederà a coinvolgere il DPO per il necessario supporto.
In caso di Data Breach il Responsabile del trattamento è tenuto a fornire la necessaria assistenza secondo le modalità definite nell'Atto di Nomina sottoscritto con quest'ultimo.

12. Procedura per l'esercizio dei diritti degli Interessati

Il GDPR riconosce agli interessati una serie di specifici diritti che gli stessi possono esercitare rivolgendo la propria richiesta al Titolare.
In particolare, gli Interessati, al ricorrere dei relativi presupposti, hanno diritto di richiedere al Titolare di:

- accedere ai propri dati e ricevere informazioni relative ai trattamenti effettuati dal Titolare (Art. 15 GDPR);
- ottenere la rettifica dei Dati personali inesatti che lo riguardano (Art. 16 GDPR);
- richiedere la cancellazione dei propri dati (Art. 17 GDPR);
- ottenere, ove consentito, la limitazione del trattamento (Art. 18 GDPR);
- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i Dati personali che lo riguardano (Art. 20 GDPR);
- opporsi in qualsiasi momento al trattamento dei Dati personali che lo riguardano (Art. 21 GDPR);
- 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 GDPR).

Da ultimo, il GDPR conferisce agli Interessati il diritto di proporre reclamo all'Autorità ai sensi dell'art. 77 GDPR nel caso in cui l'Interessato ritenga che il trattamento che lo riguardi violi le Leggi sulla protezione dei dati.
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 degli Interessati finalizzata ad individuare le modalità attraverso le quali gli stessi 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 Privacy Responsible al fine di consentire allo stesso la corretta gestione delle richieste presentate dagli Interessati.
Il Responsabile del trattamento è tenuto ad assistere il Titolare secondo le modalità definite nell'Atto di Nomina sottoscritto con quest'ultimo.

13. Registro dei Trattamenti

L'art. 30 GDPR prevede che ogni Titolare e, ove applicabile, il suo rappresentante tengano un registro delle attività di Trattamento svolte sotto la propria responsabilità. Il Registro dei Trattamenti è tenuto in forma scritta, anche in formato elettronico.
Tale Registro dei Trattamenti contiene tutte le seguenti informazioni:

- il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del contitolare del Trattamento, del rappresentante del Titolare del Trattamento e del responsabile della protezione dei dati;
- le finalità del Trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi o organizzazioni internazionali;

- 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 e, per i trasferimenti di cui all'art. 49, par. 2 GDPR, la documentazione delle garanzie adeguate,
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'ente ai sensi dell'art. 32 GDPR.

La Società ha provveduto ad implementare il Registro dei Trattamenti finalizzato a mappare le diverse operazioni di trattamento dei Dati personali effettuate in qualità di Titolare e/o Responsabile del trattamento.
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 Privacy Responsible è responsabile della corretta tenuta del Registro dei Trattamenti, nonché della sua integrazione ed aggiornamento. A tale riguardo, i Data Manager, su richiesta, sono tenuti ad assistere il Privacy Responsible al fine di espletare le predette funzioni inerenti la tenuta del Registro dei Trattamenti.
Il Privacy Responsible, con il supporto dei Data Manager e/o del Responsabile del Trattamento aggiorna il Registro dei Trattamenti con cadenza annuale e/o al verificarsi di nuovi Trattamenti e/o modifiche ai Trattamenti esistenti.
Il Responsabile tiene un registro di tutte le categorie di attività relative al Trattamento svolte per conto del Titolare, contenente le informazioni di cui all'art. 30 comma 2 del GDPR.
Il DPO verifica periodicamente lo stato di aggiornamento del Registro coinvolgendo, se del caso, il Data Manager di riferimento.

14. 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 dal momento della progettazione del Trattamento stesso. Tutte le volte in cui un determinato tipo di Trattamento dei Dati personali, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare – per il tramite del Privacy Responsible – 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 sulla protezione dei dati 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 sulla protezione dei dati 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 sulla protezione dei dati, i Destinatari sono tenuti ad assistere il Privacy Responsible fornendo tutte le informazioni necessarie ai fini della valutazione.
Il Privacy Responsible è tenuto a conservare, sotto la sua responsabilità, tutta la documentazione inerente, conseguente ed accessoria alla valutazione d'impatto.
La valutazione d'impatto deve contenere almeno:

- 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 perseguite;
- 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.

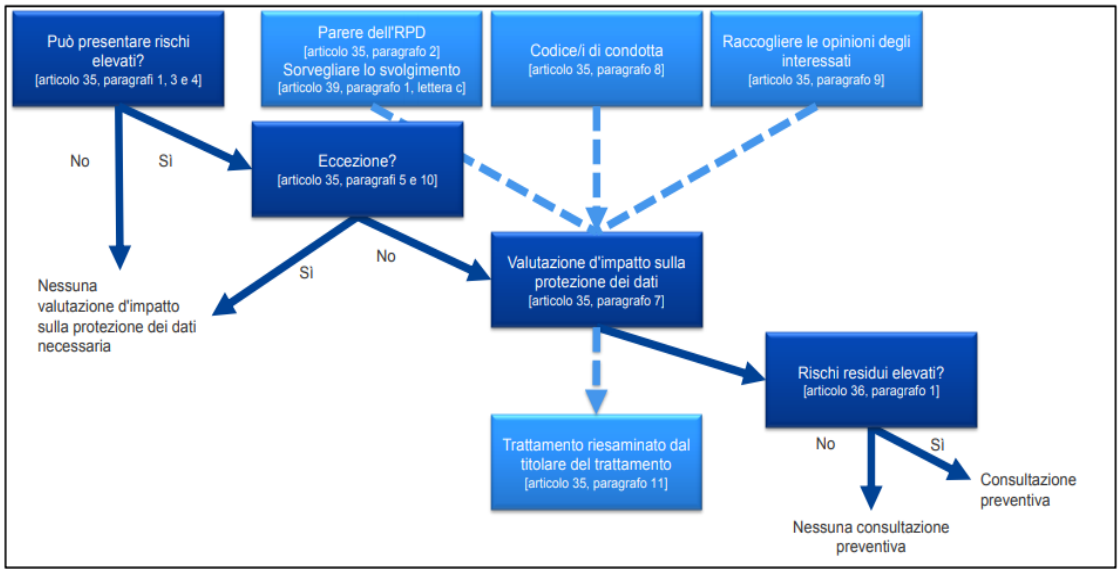
Il Privacy Responsible, con il supporto delle funzioni coinvolte nel Trattamento, effettua la Valutazione di Impatto utilizzando il format adottato dal Titolare.

In ogni caso, il Titolare, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il DPO il quale è tenuto a formulare il proprio parere e/o raccomandazione in relazione al Trattamento/ai Trattamenti oggetto di Valutazione di Impatto.

Qualora all'esito della valutazione d'impatto sulla protezione dei dati risulti che il Trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il Titolare del trattamento ritiene che il rischio in parola non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e di costi di attuazione allora il Titolare dovrà ricorrere alla **consultazione preventiva dell'Autorità di Controllo** ai sensi dell'art. 36 GDPR.

Il Responsabile del trattamento, se del caso, assiste il Titolare nello svolgimento della valutazione di impatto secondo le modalità definite nell'Atto di Nomina sottoscritto con quest'ultimo nonché nel Modello Privacy.

14.1 Flow Chart Valutazione d'impatto sulla protezione dei dati



15. Formazione

Per un efficace funzionamento del Modello, la formazione dei Data Manager e degli Autorizzati è gestita dal Privacy Responsible in accordo con il DPO.

In particolare, i corsi di formazione hanno ad oggetto il Modello, il Codice di Condotta, le Procedure 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, i partecipanti sono sottoposti ad un test finalizzato a valutare il grado di apprendimento conseguito e ad orientare ulteriori interventi formativi.

La partecipazione ai corsi di formazione è obbligatoria per tutto il personale in servizio presso la Società coinvolto nelle operazioni di Trattamento. 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.

L'attività di formazione è promossa con cadenza periodica da parte del Titolare. In caso di assunzione di una nuova risorsa nominata quale Autorizzato, la formazione in materia di tutela dei dati personali deve essere svolta entro i primi sei mesi dall'inserimento all'interno dell'organizzazione del Titolare.

16. Inosservanza del Modello Organizzativo Privacy

Si porta a conoscenza di tutti i Destinatari che il presente Modello, il Codice di Condotta e le Procedure hanno carattere vincolante per i Destinatari.

Eventuali violazioni del presente Modello, del Codice di Condotta e delle Procedure 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 dei soggetti terzi (e.g. fornitori) 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 del Modello, del Codice di Condotta e delle Procedure.

17. Contatti

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

- ✓ Privacy Responsible
  - E-mail: legal@burgerking.it
- ✓ DPO:
  - E-mail: dpo@burgerking.it