DATA BREACH POLICY

1. INTRODUZIONE

Il GDPR introduce in capo agli enti che pongono in essere attività di trattamento di Dati personali, l'obbligo di notificare all'Autorità le violazioni 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 dalla società **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 (di seguito, la "**Società**" o il "**Titolare**") e in linea con i principi di *risk management,* la Società ha ritenuto necessario adottare la presente Procedura al fine di disciplinare le opportune modalità di gestione dei Data Breach, individuando le azioni da compiere da parte dei soggetti coinvolti nelle operazioni di trattamento di Dati personali di cui la stessa è Titolare del trattamento.

I termini indicati con l'iniziale maiuscola, ove non diversamente definiti, avranno il significato loro attribuito nel Modello Organizzativo Privacy adottato dalla Società.

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 Privacy Responsible o al Titolare, 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;

- l'Amministratore di sistema è tenuto a supportare il Privacy Responsible e il Titolare nello svolgimento delle attività di verifica finalizzate ad accertare la natura della violazione nonché gli impatti e i rischi derivanti dalla stessa;

- il DPO è tenuto a supportare il Titolare e il Privacy Responsible nella gestione dell'eventuale Data Breach e a formulare pareri e raccomandazioni sulle misure rimediative da implementare a seguito dell'evento.

- il Privacy Responsible 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, fornire supporto al Titolare per effettuare le segnalazioni all'Autorità e/o le comunicazioni agli Interessati nonché a manutenere il registro delle violazioni segnalate di cui all'Annex 1.

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 integrare 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 7 che segue.

Al fine di coadiuvare il Titolare il Privacy Responsible nella gestione tempestiva delle attività di notifica della violazione dei Dati personali all'Autorità, il Destinatario dovrà primariamente effettuare la segnalazione scrivendo all'indirizzo e-mail legal@burgerking.it, indicando gli 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 6 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 7.

3.2 Analisi preliminare ed elaborazione del Severity Assessment e Registro dei Data Breach

Qualora venga segnalata una possibile violazione dei Dati personali, il Privacy Responsible, con il supporto del DPO, deve svolgere le necessarie indagini ed avviare un'analisi preliminare provvedendo a compilare il Severity Assessment di cui all'Annex 1.

Il Privacy Responsible è tenuto a documentare le risultanze delle anzidette indagini al fine di consentire al Titolare 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 Responsible, sentito il DPO, provvede ad archiviare l'incidente. In ogni caso, il Privacy Responsible è tenuto a dare evidenza del c.d. falso positivo all'interno del Registro dei Data Breach, di cui all'Annex 1, nella apposita sezione dedicata agli "incidenti infondati".

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

3.3 Norme di condotta per il Titolare e il Privacy Responsible

3.3.1 Notifica all'Autorità

Nel caso in cui la violazione di sicurezza **non** si dimostri idonea a rappresentare un rischio per i diritti e le libertà degli Interessati coinvolti, il Privacy Responsible, sentito il DPO, procede alla registrazione della violazione e all'archiviazione di quanto segnalato avvalendosi del registro di cui all'Annex 1.

Qualora la violazione **possa comportare un rischio per i diritti e le libertà delle persone fisiche**, il Titolare, se del caso con il supporto del Privacy Responsible, provvede ad effettuare la notifica all'Autorità nel limite delle 72 ore successive al momento in cui si è avuta consapevolezza dell'avvenuta violazione. Qualora la notifica all'Autorità non sia effettuata entro 72 ore, la stessa deve essere corredata dei motivi del ritardo.

Il DPO supporta il Titolare ad effettuare la Notifica.

Come strumento di ulteriore supporto per definire la necessità o meno di effettuare la notifica all'Autorità, il Titolare può avvalersi del tool messo a disposizione dall'Autorità disponibile al seguente link https://servizi.gpdp.it/databreach/s/self-assessment.

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 DPO (se nominato) 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, il Titolare può effettuare una notifica preliminare, riservando di fornire le ulteriori informazioni in fasi successive senza ulteriore ingiustificato ritardo.

Qualora successivamente all'avvenuta notifica, emergessero degli elementi e/o il Titolare implementasse misure tali da rendere improbabile un rischio per i diritti e le libertà degli interessati, il Titolare potrà annullare la notifica precedentemente inviata.

Il Titolare, con il supporto del Privacy Responsible, 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 è suscettibile di presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il Titolare, con il supporto del Privacy Responsible e sentito il DPO, comunica 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 DPO 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;

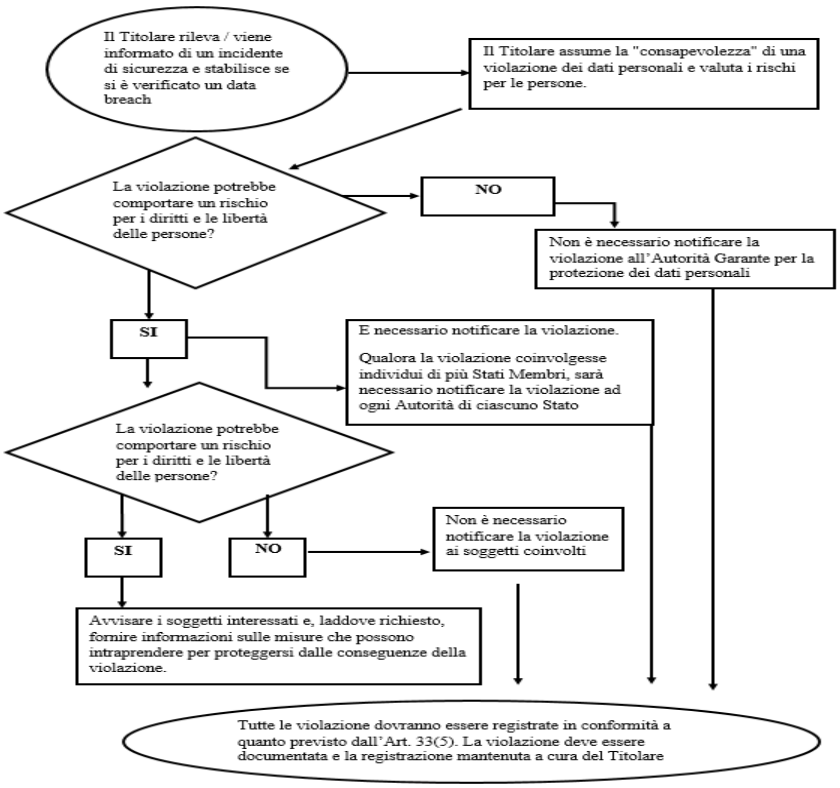
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati;

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 Titolare, con il supporto del Privacy Responsible, provvede alla registrazione della violazione avvalendosi del registro di cui all'Annex 1.

4. FLOW CHART DATA BREACH POLICY

Si riporta nel seguito una sintesi della procedura di gestione della notifica all'Autorità.



5. MISURE RIMEDIATIVE

A prescindere dalla gravità del Data Breach e/o dell'incidente verificatosi il Privacy Responsible con il supporto del DPO definisce le azioni rimediative/di miglioramento finalizzate a mitigare il rischio derivante dalla violazione e/o a prevenire il verificarsi di eventi simili.

Il DPO monitora l'effettiva implementazione delle misure pianificate.

6. 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		**Dati anagrafici / codice fiscale**
		Dati di accesso e di identificazione *(username, password, etc.)*
		Dati relativi a minori

oggetto di violazione		**Particolari categorie di dati** *(origine razziale 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		

7. CONTATTI

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

- ✓ Privacy Responsible:

- E-mail: legal@burgerking.it

✓ DPO:

- E-mail: dpo@burgerking.it

Allegati

Annex 1 Severity Assessment & Data Breach Record