

# **Norme vincolanti d'impresa Sodexo**

**Processor Policy**



# Indice

<b>1. Introduzione generale .....</b>	<b>5</b>
Introduzione .....	6
Cos'è il GDPR .....	7
Il GDPR ha un impatto sui flussi transfrontalieri di Dati personali all'interno di Sodexo? .....	7
Qual è l'ambito di applicazione e lo scopo delle BCR Sodexo? .....	8
Cosa comporta in pratica per i Dati personali raccolti e utilizzati in Europa? .....	10
Ruoli nell'ambito della Protezione dei Dati personali.....	10
Informazioni aggiuntive .....	11
<b>2. Le Norme.....</b>	<b>12</b>
NORMA 1 – CONFORMITÀ A BCR, GDPR E NORMATIVA LOCALE APPLICABILE .....	13
NORMA 2 – GARANTIRE LICEITÀ, CORRETTEZZA E TRASPARENZA .....	14
NORMA 3 – GARANTIRE LA LIMITAZIONE DELLA FINALITÀ .....	14
NORMA 4 – GARANTIRE LA MINIMIZZAZIONE DEI DATI .....	15
NORMA 5 – GARANTIRE L'ACCURATEZZA .....	15
NORMA 6 – GARANTIRE LA LIMITAZIONE DELLA CONSERVAZIONE .....	16
NORMA 7 – ADOTTARE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADEGUATE .....	16
NORMA 8 – SALVAGUARDIA DELL'USO DEI DATI PERSONALI SENSIBILI E DI ALTRE CATEGORIE PARTICOLARI DI DATI PERSONALI .....	18
NORMA 9 – MANTENERE REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI ..	19
NORMA 10 – RISPETTO DEI DIRITTI DEGLI INTERESSATI .....	20
NORMA 11 – RISPETTARE LE CONDIZIONI PER IL PROCESSO DECISIONALE INDIVIDUALE AUTOMATIZZATO E LA PROFILAZIONE E IMPLEMENTARE LE MISURE DI SALVAGUARDIA ADEGUATE .....	21
NORMA 12 – TRASPARENZA E INFORMAZIONE DELL'INTERESSATO.....	21
NORMA 13 – GARANTIRE UNA PROTEZIONE ADEGUATA PER I TRASFERIMENTI TRANSFRONTALIERI DI DATI PERSONALI .....	21
NORMA 14 – ADOTTARE LA PRIVACY FIN DALLA PROGETTAZIONE E DI DEFAULT ..	22
NORMA 15 – ESECUZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) .....	22
NORMA 16 – FORMAZIONE E SENSIBILIZZAZIONE .....	23
NORMA 17 – GESTIONE DEI DIRITTI DI PROTEZIONE DEI DATI .....	24
NORMA 18 – VALUTAZIONE DELLA COMPLIANCE: PROGRAMMA DI AUDIT .....	24
NORMA 19 – MONITORAGGIO DELL'APPLICAZIONE DELLE BCR.....	25
NORMA 20 – GLOBAL DATA PROTECTION OFFICE E RETE DEI REFERENTI UNICI LOCALI .....	26
NORMA 21 – DIRITTI DEI BENEFICIARI TERZI.....	27

NORMA 22 – RESPONSABILITÀ .....	30
<b>3. Disposizioni finali .....</b>	<b>31</b>
NORMA 23 – AZIONI IN CASO DI LEGISLAZIONE O PRASSI NAZIONALI CHE IMPEDISCANO IL RISPETTO DELLE BCR – RICHIESTA GIURIDICAMENTE VINCOLANTE DI DIVULGAZIONE DEI DATI PERSONALI.....	32
NORMA 24 – COOPERAZIONE CON LE AUTORITÀ DI CONTROLLO .....	35
NORMA 25 – AGGIORNAMENTO DELLE BCR .....	36
NORMA 26 – VINCOLATIVITÀ DELLE BCR .....	36
<b>4. Appendici .....</b>	<b>38</b>
Appendice 1 – Definizioni.....	40
Appendice 2 – Politica globale di raccolta e conservazione dei dati (Responsabile del trattamento).....	43
Appendice 3 – Procedura di cooperazione delle BCR.....	46
Appendice 4 – Procedura di aggiornamento delle BCR .....	47
Appendice 5 – Politica globale sulla protezione dei dati di Sodexo .....	49
Appendice 6 – Politica globale di gestione dei diritti per la protezione dei dati.....	50
Appendice 7 – Descrizione dell'ambito di applicazione materiale della Processor Policy ...	51

In questo documento, “Sodexo” si riferisce collettivamente alle entità Sodexo che hanno aderito alla Processor Policy delle Norme vincolanti d'impresa (“BCR”) tramite la sottoscrizione di un accordo infragruppo (la/e “entità Sodexo” o “membri della Processor Policy”)<sup>1</sup>.

## **DESTINATARI:**

Tutti i dipendenti Sodexo (compresi i nuovi assunti e chiunque agisca per conto di Sodexo, in qualità di consulente e singolo appaltatore).

## **PUBBLICATO DA:**

Ufficio legale del Gruppo Sodexo (Global Data Protection Office)

## **VERSIONE:**

1.0

## **SOSTITUISCE:**

La Processor Policy contenuta nelle Norme vincolanti d'impresa (“BCR”) Sodexo sostituisce tutte le politiche e le informative sulla protezione dei dati di Sodexo esistenti alla data di entrata in vigore, nella misura in cui affrontano le stesse tematiche e non sono coerenti con la presente politica.

## **DATA DI ENTRATA IN VIGORE:**

21 dicembre 2023

In caso di discrepanze tra la versione inglese della presente Politica e una versione tradotta, prevarrà la versione inglese.

***Copyright Sodexo, tutti i diritti riservati.***

---

<sup>1</sup> Per entità Sodexo si intende qualsiasi controllata del Gruppo Sodexo (cioè, una o più entità direttamente o indirettamente controllate da o sotto controllo congiunto con Sodexo SA, come definito dall'Articolo L. 233-3 del Codice di Commercio francese) soggetta alle Norme vincolanti d'impresa Sodexo.

# 01

## Introduzione generale



## Introduzione

Sodexo ha definito un quadro di riferimento e una disposizione chiara in materia di protezione dei dati personali nell'ambito del Global Data Protection Compliance Program di Sodexo, nella fattispecie le Norme vincolanti d'impresa Sodexo ("BCR" o "BCR Sodexo").

Le BCR Sodexo sono incorporate all'interno del Codice di condotta per l'integrità aziendale di Sodexo. In base a questo codice, tutti i dipendenti sono responsabili e tenuti a rispettare e proteggere la privacy e le informazioni riservate dei loro stakeholder, ivi compresi candidati all'assunzione, dipendenti, clienti, consumatori/beneficiari, fornitori/venditori, appaltatori/subappaltatori e altre terze parti, in conformità alle leggi e ai regolamenti applicabili.

Le BCR sono costituite dalle due politiche seguenti, incluse le relative appendici:

- la Politica delle Norme vincolanti d'impresa sulla protezione dei dati per il titolare del trattamento ("Controller Policy" o "BCR-C");
- la Politica delle Norme vincolanti d'impresa sulla protezione dei dati per il responsabile del trattamento ("Processor Policy" o "BCR-P").

Le BCR Sodexo sono state realizzate al fine di stabilire l'approccio di Sodexo per dimostrare, mantenere e monitorare la conformità alla normativa europea<sup>2</sup> sulla protezione dei dati, come stabilito dal Regolamento Generale sulla Protezione dei Dati (il "GDPR")<sup>3</sup> in tutto il Gruppo Sodexo e, in particolare, ai flussi transfrontalieri di Dati personali tra le entità Sodexo.

La presente Processor Policy si applica a tutte le entità Sodexo e ai relativi dipendenti (compresi i nuovi assunti), nonché a qualsiasi persona che agisca per loro conto (consulenti e singoli appaltatori). Essa si compone di 26 Norme che Sodexo deve osservare e rispettare durante la raccolta e l'elaborazione dei Dati personali in qualità di Responsabile del trattamento e anche durante il trasferimento dei dati ai titolari o ai responsabili del trattamento all'interno del Gruppo Sodexo.

I termini con iniziale maiuscola utilizzati nella presente politica sono definiti nell'Appendice 1.

La Processor Policy sarà pubblicata sul sito web accessibile all'indirizzo [www.sodexo.com](http://www.sodexo.com).

---

<sup>2</sup> Ai fini delle presenti BCR, per Europa si intende l'UE/il SEE e la Svizzera e "UE" o "europeo" devono essere interpretati di conseguenza.

<sup>3</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche in materia di trattamento dei Dati personali, nonché alla libera circolazione di tali dati, che abroga la Direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati o "GDPR").

## Cos'è il GDPR

Il GDPR garantisce alle persone il diritto di controllare il modo in cui vengono utilizzati i propri Dati personali.

La raccolta e il trattamento da parte di Sodexo dei Dati personali di candidati, dipendenti, clienti, consumatori/beneficiari, fornitori/venditori, appaltatori/subappaltatori o di terze parti, siano essi attuali, passati o potenziali, sono disciplinati dal GDPR.

Ai sensi del GDPR, per Dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile (“Interessato”); per persona fisica identificabile si intende una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un identificativo come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica (“Dati personali”).

Rientra nell'ambito di applicazione del GDPR qualsiasi operazione o insieme di operazioni eseguite da Sodexo sui Dati personali raccolti dagli Interessati, con o senza l'ausilio di mezzi automatizzati, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione o messa a disposizione in altro modo, l'allineamento o la combinazione, la limitazione, la cancellazione o la distruzione (“Trattamento” o “Trattamento dei Dati personali”).

Il GDPR opera una distinzione tra “titolare del trattamento” e “responsabile del trattamento”. Il titolare del trattamento determina, da solo o congiuntamente ad altri, le finalità e i mezzi del Trattamento dei Dati personali (“Titolare del trattamento”). Il responsabile del trattamento, invece, tratta i Dati personali per conto del titolare del trattamento (“Responsabile del trattamento”).

Sodexo agisce come Titolare del trattamento per le questioni in cui Sodexo determina le finalità e i mezzi del trattamento dei dati, e agisce in qualità di Responsabile del trattamento quando elabora i Dati personali in base alle specifiche disposizioni del Titolare del trattamento.

## Il GDPR ha un impatto sui flussi transfrontalieri di Dati personali all'interno di Sodexo?

Il GDPR si applica non solo alle entità Sodexo con sede nell'UE/nel SEE, ma anche alle entità Sodexo con sede al di fuori dell'UE/del SEE qualora: (a) queste offrano beni o servizi a Interessati europei; oppure (b) il Trattamento dei Dati personali effettuato comporti il monitoraggio del comportamento di Interessati europei.

Il GDPR non consente i trasferimenti transfrontalieri dei Dati personali a Paesi al di fuori dell'Europa che non garantiscono un livello adeguato di protezione dei dati. Secondo la

Commissione europea o le autorità di controllo europee, alcuni Paesi in cui opera Sodexo non offrono un livello adeguato di protezione dei diritti e delle libertà fondamentali delle persone fisiche in relazione alle attività di trattamento.

## Qual è l'ambito di applicazione e lo scopo delle BCR Sodexo?

Lo scopo delle presenti BCR è quello di fornire un'informativa chiara in materia di protezione dei Dati personali al fine di garantire un adeguato livello di tutela per tutti gli Interessati in conformità alle disposizioni del GDPR.

La Processor Policy prevede 26 Norme fondate e interpretate in conformità al GDPR, cui devono attenersi tutti i dipendenti Sodexo (ivi compresi i nuovi assunti e qualsiasi persona che agisca per conto di Sodexo, come consulenti e singoli appaltatori) dei membri della Processor Policy in riferimento al trattamento dei Dati personali, a prescindere dal Paese in cui operino.

La presente Processor Policy riguarda il Trattamento di tutti i Dati personali di clienti, consumatori/beneficiari di Sodexo, siano essi attuali, passati o potenziali, nonché il Trattamento per conto di un Cliente.

L'ambito geografico della Processor Policy è il seguente: la Processor Policy inquadra tutti i flussi di Dati personali elaborati da Sodexo per conto di un Cliente per attività di trattamento all'interno del Gruppo, indipendentemente dall'origine dei Dati personali.

L'ambito di applicazione materiale della Processor Policy è descritto nell'Appendice 7.

— I Paesi dell'UE/del SEE sono i seguenti:

- Austria
- Belgio
- Bulgaria
- Cipro
- Repubblica Ceca
- Danimarca
- Finlandia
- Francia
- Germania
- Ungheria
- Irlanda
- Italia
- Lussemburgo
- Paesi Bassi
- Norvegia



- Polonia
- Portogallo
- Romania
- Spagna
- Svezia

■ I Paesi terzi sono i seguenti:

- Algeria
- Australia
- Brasile
- Canada
- Cile
- Cina continentale
- Colombia
- Costa Rica
- India
- Indonesia
- Israele
- Giappone
- Malesia
- Messico
- Marocco
- Myanmar
- Nuova Zelanda
- Oman
- Panama
- Perù
- Filippine
- Repubblica di Corea
- Singapore
- Sudafrica
- Sri Lanka
- Svizzera
- Thailandia
- Tunisia
- Turchia
- Uruguay
- Emirati Arabi Uniti

- Regno Unito
- Stati Uniti d'America
- Venezuela
- Vietnam

## Cosa comporta in pratica per i Dati personali raccolti e utilizzati in Europa?

Gli Interessati i cui Dati personali sono trattati in qualsiasi Paese da un'entità Sodexo che agisce in qualità di Responsabile del trattamento e trasferiti all'interno del Gruppo Sodexo hanno il diritto di sporgere reclamo o ottenere rimedi giuridici e ricorsi appropriati e, se del caso, ricevere un risarcimento, come stabilito dalla Norma 21, per qualsiasi violazione delle norme contenute nella Processor Policy:

- (i) che sono direttamente opponibili al Responsabile del trattamento (obbligo di rispettare le istruzioni del Titolare del trattamento, di implementare misure di sicurezza tecniche e organizzative adeguate, di rispettare le condizioni di ingaggio di un sub-responsabile, di collaborare e assistere il Titolare del trattamento a rispettare e dimostrare la conformità al GDPR, la facilità di accesso alle BCR, la trasparenza sui casi in cui la legislazione impedisce il rispetto delle BCR, diritto di presentare un reclamo attraverso i rispettivi meccanismi interni, responsabilità e doveri di cooperazione con le Autorità di controllo); e
- (ii) che sono opponibili al Responsabile del trattamento nel caso in cui l'Interessato non sia in grado di presentare un reclamo nei confronti del Titolare del trattamento (obbligo di rispettare le BCR, diritti di beneficiari terzi, responsabilità e onere della prova a carico di Sodexo e non dell'Interessato, facilità di accesso alle BCR e trasparenza, gestione dei reclami, cooperazione con le Autorità di controllo, elenco di entità soggette alle BCR, obbligo di cooperazione con il Titolare del trattamento, trasparenza sui casi in cui la legislazione impedisce a Sodexo di rispettare le BCR e i principi in materia di Protezione dei dati).

## Ruoli nell'ambito della Protezione dei Dati personali

Il Group Data Protection Officer di Sodexo, insieme al Global Data Protection Office e alla rete dei Referenti unici locali per la protezione dei dati ("Global Data Protection Network") sono incaricati di monitorare la conformità interna alla Processor Policy e a qualsiasi altra politica e procedura sottesa.

I titolari di attività (designati come incaricati della Protezione dei dati nell'ambito di funzioni aziendali, servizi operativi e segmenti) e i proprietari delle applicazioni IT sono responsabili di

supervisionare la conformità alla presente politica da parte delle entità Sodexo all'interno del proprio perimetro e su base giornaliera.

## Informazioni aggiuntive

In qualità di multinazionale con sede in Francia, Sodexo SA è una delle entità centrali del Gruppo Sodexo che ha richiesto, per sé e per conto delle entità Sodexo del Gruppo Sodexo, l'approvazione dell'Autorità di controllo competente, ossia l'autorità francese (*Commission Nationale de l'Informatique et des Libertés* o CNIL; [www.cnil.fr](http://www.cnil.fr)).

In caso di domande relative alle disposizioni della Processor Policy, ai propri diritti ai sensi della presente politica o a qualsiasi altra questione relativa alla protezione dei dati, è possibile contattare il Group Data Protection Officer di Sodexo, il quale si occuperà della questione o la inoltrerà ai Referenti unici locali per la protezione dei dati o ai titolari di attività o ai responsabili IT all'interno di Sodexo, al seguente indirizzo:

Group Data Protection Officer:

e-mail: [dpo.group@sodexo.com](mailto:dpo.group@sodexo.com)

Indirizzo:

Group Data Protection Officer  
Team legale del Gruppo  
Sodexo SA  
255 quai de la Bataille de Stalingrad  
92300, Issy-les-Moulineaux  
Francia

Il Group Data Protection Officer è responsabile di garantire che le modifiche alla presente Processor Policy siano comunicate alle entità Sodexo e alle persone i cui Dati personali sono trattati da Sodexo tramite il sito web di Sodexo all'indirizzo [www.sodexo.com](http://www.sodexo.com).

# 02

## Le Norme



Le norme della Processor Policy sono suddivise in due sezioni:

- la Sezione A tratta le Norme sulla Protezione dei dati che Sodexo deve osservare per la raccolta e il trattamento dei Dati personali;
- la Sezione B tratta degli impegni concreti assunti da Sodexo nei confronti delle Autorità di controllo europee per garantire la vincolatività e l'efficacia della Processor Policy.

## Sezione A

### NORMA 1 – CONFORMITÀ A BCR, GDPR E NORMATIVA LOCALE APPLICABILE

***NORMA 1.A – Sodexo si attiene in primo luogo alle disposizioni previste dalla Processor Policy, stabilite in conformità al GDPR e alla normativa locale applicabile, la quale richiederebbe un livello di protezione più elevato per i Dati personali, laddove esistente.***

Sodexo si attiene alle disposizioni della Processor Policy, in conformità al GDPR e alla normativa locale applicabile, se presente.

Laddove la normativa locale applicabile richieda un livello di protezione dei Dati personali più elevato rispetto al GDPR, tale normativa prevarrà sulla Processor Policy.

In assenza di una normativa specifica o laddove quest'ultima non soddisfi gli standard stabiliti dalle BCR, Sodexo tratterà i Dati personali in conformità alla Processor Policy.

***NORMA 1.B – Sodexo collabora e assiste i Titolari del trattamento nell'adempimento dei loro obblighi ai sensi del GDPR e della normativa locale applicabile, se del caso, che richieda un livello di protezione più elevato per i Dati personali, in tempi ragionevoli e nella misura ragionevolmente possibile.***

Sodexo, in un tempo ragionevole e nella misura ragionevolmente possibile, come richiesto dai suoi obblighi contrattuali o da altri documenti vincolanti con un Titolare del trattamento (un Cliente), collabora e assiste il Titolare del trattamento (un Cliente) nell'impegno di quest'ultimo a essere conforme al GDPR e alla normativa locale applicabile.

## NORMA 2 – GARANTIRE LICEITÀ, CORRETTEZZA E TRASPARENZA

**REGOLA 2.A – Sodexo assiste il Titolare del trattamento nell'adempimento dei suoi obblighi di liceità, correttezza e trasparenza.**

Sodexo assiste il Titolare del trattamento (un Cliente) su richiesta.

Inoltre, Sodexo assiste e collabora con il Titolare del trattamento per rispondere alle richieste e ai reclami degli Interessati (cfr. Norme 25 e 17), per informare le altre parti coinvolte nel Trattamento dei Dati personali, come appropriato, affinché i Dati personali degli Interessati siano accurati e aggiornati (cfr. Norma 5) e per rispondere a qualsiasi accertamento o indagine da parte delle Autorità di controllo.

**REGOLA 2.B - Sodexo raccoglie e tratta i Dati Personali solo per conto e secondo le istruzioni del Titolare del Trattamento.**

Sodexo raccoglie ed elabora i Dati personali solo per conto e in conformità alle istruzioni documentate (legittime) ricevute dal Titolare del trattamento (un Cliente), come specificato nell'accordo per la fornitura di servizi, nel contratto e in qualsiasi altro documento vincolante con il Titolare del trattamento (un Cliente).

Qualora Sodexo non sia in grado di rispettare questa Norma, provvederà ad informare tempestivamente il Titolare del trattamento. In tal caso, il Titolare del trattamento ha il diritto di interrompere il rapporto contrattuale con Sodexo per quanto riguarda il Trattamento dei Dati personali, alle condizioni stabilite nell'accordo per la fornitura di servizi, nel contratto o in qualsiasi altro documento vincolante con il Titolare del trattamento (un Cliente). Qualora sia probabile una modifica delle condizioni di Trattamento dei Dati personali durante l'esecuzione dei servizi forniti da Sodexo, quest'ultima informerà il Titolare del trattamento, il quale avrà la possibilità di opporsi alla modifica o di risolvere il contratto o qualsiasi altro documento vincolante in questione prima dell'attuazione di tale modifica.

## NORMA 3 – GARANTIRE LA LIMITAZIONE DELLA FINALITÀ

**REGOLA 3 – Sodexo tratta i Dati personali per conto del Titolare del trattamento per una finalità nota, pertinente e legalmente fondata determinata dal Titolare del trattamento.**

Sodexo tratta i Dati personali per conto del Titolare del trattamento, per finalità specifiche, esplicite e legittime, secondo le istruzioni del Titolare del trattamento, e non li elabora

ulteriormente secondo modalità incompatibili con tali finalità, anche per quanto riguarda il trasferimento di Dati personali in un Paese terzo, a meno che non sia richiesto dal GDPR o dalla normativa locale applicabile che richiede un livello di protezione più elevato per i Dati personali e a cui Sodexo è soggetta in qualità di Responsabile del trattamento. In tal caso, Sodexo informa il Titolare del trattamento di tale requisito legale prima che avvenga il trattamento, a meno che la legge non vieti tale informazione per importanti ragioni di interesse pubblico. In altri casi, se Sodexo, in qualità di Responsabile del trattamento, non è in grado di fornire per qualsiasi motivo tale conformità, si impegna ad informare tempestivamente il Titolare del trattamento della propria incapacità in tal senso; il Titolare del trattamento ha in tal caso il diritto di sospendere i trasferimenti dei Dati personali in questione e/o di risolvere il contratto o qualsiasi altro documento vincolante.

## NORMA 4 – GARANTIRE LA MINIMIZZAZIONE DEI DATI

***NORMA 4 – Sodexo tratta solo i Dati personali rilevanti e necessari per l'esecuzione dei servizi.***

Sodexo identifica il quantitativo minimo di Dati personali necessari per adempiere correttamente alle finalità dei servizi, come stabilito nell'accordo per la fornitura di servizi, nel contratto e in qualsiasi altro documento vincolante stipulato con il Titolare del trattamento (un Cliente).

## NORMA 5 – GARANTIRE L'ACCURATEZZA

***NORMA 5 – Sodexo assiste il Titolare del trattamento affinché i Dati personali siano accurati e, se necessario, aggiornati.***

Sodexo e i suoi eventuali sub-responsabili agiscono su istruzioni del Titolare del trattamento (un Cliente) al fine di assistere il Titolare del trattamento nell'adempimento del suo obbligo di mantenere i Dati personali accurati e, se necessario, aggiornati, al fine di aggiornare, correggere o cancellare i Dati personali.

In quanto Responsabile del trattamento, Sodexo informa ogni entità Sodexo a cui sono stati divulgati i Dati personali di qualsiasi rettifica o cancellazione dei Dati personali.

Quando richiesto, su istruzione del Titolare del trattamento, come previsto dalle disposizioni del contratto o altro documento vincolante stipulato con tale Titolare, Sodexo e i suoi eventuali sub-responsabili adotteranno le misure necessarie affinché i Dati personali siano cancellati o resi anonimi dal momento in cui il modulo di identificazione non è più necessario.

In quanto Responsabile del trattamento, Sodexo informa ogni entità Sodexo a cui sono stati divulgati i Dati Personali di qualsiasi cancellazione o anonimizzazione dei dati.

## NORMA 6 – GARANTIRE LA LIMITAZIONE DELLA CONSERVAZIONE

***NORMA 6 – Sodexo assiste il Titolare del trattamento a conservare i Dati personali per il tempo necessario.***

I Dati personali sono sempre conservati e/o cancellati e/o anonimizzati secondo le istruzioni del Titolare del trattamento (a condizione che tali istruzioni non siano in conflitto con la normativa locale applicabile) e in linea con la Politica globale sulla raccolta e sulla conservazione dei dati di Sodexo (Appendice 2). Sodexo elimina i Dati personali solo in modo sicuro, in conformità con la Politica di sicurezza delle informazioni e dei sistemi del Gruppo<sup>4</sup>.

Al termine della fornitura dei servizi relativi al Trattamento dei dati personali, Sodexo in qualità di Responsabile del trattamento e i suoi eventuali sub-responsabili, a scelta del Titolare del trattamento, eliminano, anonimizzano tutti i Dati personali trasferiti o restituiscono le relative copie al Titolare del trattamento, a meno che la normativa locale applicabile, ad esempio la legislazione UE/SEE, non richieda la conservazione dei Dati personali trasferiti. In tal caso, Sodexo informa il Titolare del trattamento e garantisce che assicurerà la riservatezza dei Dati personali trasferiti e non tratterà più attivamente questi ultimi.

## NORMA 7 – ADOTTARE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADEGUATE

***NORMA 7.A – Sodexo aderisce alla Politica di sicurezza delle informazioni e dei sistemi del Gruppo Sodexo e implementa le misure tecniche e organizzative secondo quanto specificato nell'accordo per la fornitura di servizi, nel contratto e in qualsiasi altro documento vincolante stipulato con il Titolare del trattamento, in conformità con la normativa locale applicabile di quest'ultimo.***

Sodexo adempie ai requisiti contenuti nella Politica di sicurezza delle informazioni e dei sistemi del Gruppo Sodexo<sup>5</sup>, modificata e aggiornata di volta in volta, insieme a qualsiasi altra misura di

---

<sup>4</sup> Documento interno

<sup>5</sup> Documento interno



sicurezza, integrità e riservatezza pertinente a un'area o funzione aziendale, nonché alle misure di sicurezza tecniche e organizzative specificate nel contratto o in qualsiasi altro documento vincolante stipulato con il Titolare del trattamento (un Cliente), che proteggeranno i Dati personali dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati, in aggiunta alla normativa locale applicabile del Titolare del trattamento.

In funzione della natura del Trattamento dei Dati personali, queste misure tecniche e organizzative possono includere la crittografia dei Dati personali, revisioni continue delle misure di sicurezza, strutture di ridondanza e di back-up e test di sicurezza regolari.

***NORMA 7.B – Sodexo nomina un sub-responsabile all'interno o all'esterno del Gruppo, previa autorizzazione scritta generale o specifica del Titolare del trattamento e in base a impegni simili a quelli stabiliti nel contratto con il Titolare del trattamento e nella Processor Policy.***

Sodexo assicura che il sub-trattamento dei dati personali all'interno del Gruppo e/o i trasferimenti successivi a sub-responsabili esterni siano eseguiti con la previa autorizzazione scritta, generale o specifica, del Titolare del trattamento, in conformità alle sue istruzioni (ad esempio, autorizzazione generale o specifica, notifica di modifica, possibilità di opporsi a qualsiasi modifica o di risoluzione del contratto) per quanto riguarda la nomina dei sub-responsabili, come stabilito dalle disposizioni dell'accordo per la fornitura di servizi, del contratto o di qualsiasi altro documento vincolante, e che il sub-trattamento sia strettamente pertinente alla finalità dell'esecuzione dei servizi.

In caso di sub-trattamento all'interno del Gruppo, i Dati personali possono essere sub-trattati da altre entità Sodexo soggette alle BCR solo previa autorizzazione scritta informata<sup>6</sup>, specifica o generale, del Titolare del trattamento.

Sodexo provvede a mettere a disposizione del Titolare del trattamento informazioni aggiornate in merito alla nomina di sub-responsabili, in conformità alle istruzioni del Titolare del trattamento concordate contrattualmente.

Laddove il Titolare del trattamento accetti la nomina di sub-responsabili, questi saranno nominati in base ad adempimenti simili a quelli stabiliti nel contratto tra Sodexo e il Titolare del trattamento, e in ogni caso in conformità alla Norma 7.B e alla Processor Policy.

---

<sup>6</sup> Informazioni sugli elementi principali (parti, Paesi, sicurezza, garanzie in caso di trasferimenti internazionali, con la possibilità di ottenere una copia del contratto utilizzato).

***NORMA 7.C – Sodexo comunica qualsiasi Violazione dei dati personali al Titolare del trattamento senza indebito ritardo, in conformità alle condizioni concordate nel contratto o in qualsiasi altro documento vincolante.***

Sodexo comunica qualsiasi Violazione dei Dati Personali al Titolare del Trattamento entro il periodo di tempo concordato con quest'ultimo per venirne a conoscenza e in ogni caso senza ritardi ingiustificati.

Sodexo assiste il Titolare del trattamento nell'identificazione della natura della Violazione dei Dati personali, delle probabili conseguenze di detta violazione, delle misure da proporre o da adottare per affrontare la Violazione dei dati personali e di qualsiasi altra richiesta di assistenza da parte del Titolare del trattamento, in conformità alle istruzioni concordate contrattualmente con lo stesso.

Inoltre, i sub-responsabili (se presenti) hanno il dovere di informare senza indebito ritardo Sodexo, che agisce in qualità di Responsabile e di Titolare del trattamento.

***NORMA 7.D – Sodexo garantisce la riservatezza dei Dati personali trattati per conto del Titolare del trattamento.***

Sodexo garantisce la riservatezza dei Dati personali trattati.

Sodexo provvede affinché tutte le persone autorizzate a trattare i Dati personali si impegnino a rispettare un adeguato obbligo di riservatezza.

## **NORMA 8 – SALVAGUARDIA DELL'USO DEI DATI PERSONALI SENSIBILI E DI ALTRE CATEGORIE PARTICOLARI DI DATI PERSONALI**

***NORMA 8 – Sodexo tratta i Dati personali sensibili e altre categorie particolari di Dati personali solo in conformità alle istruzioni legittime scritte e documentate del Titolare del trattamento e non tratta ulteriormente tali dati per altre finalità.***

Sodexo tratta i Dati personali sensibili e altre categorie speciali di Dati personali solo in conformità alle istruzioni legittime del Titolare del trattamento e non li tratta ulteriormente per altre finalità.

Qualora Sodexo non sia in grado di trattare tali Dati personali in conformità alle istruzioni del Titolare del trattamento, informerà tempestivamente il Titolare del trattamento in merito a questa sua impossibilità; in tal caso, il Titolare del trattamento avrà il diritto di risolvere il rapporto

contrattuale con Sodexo rispettando le istruzioni del Titolare del trattamento in merito alla restituzione, all'anonimizzazione e alla distruzione dei Dati personali in conformità alla Norma 6.

## NORMA 9 – MANTENERE REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO DEI DATI

***NORMA 9 – Sodexo mantiene i registri di tutte le categorie di attività di trattamento svolte per conto del Titolare del trattamento.***

Sodexo mantiene i registri delle sue attività di trattamento svolte per conto del Titolare del trattamento, compresa una descrizione generale delle misure di sicurezza implementate in relazione ai Dati personali trattati per conto del Titolare del trattamento.

Questi registri includono, in conformità all'Articolo 30(2) del GDPR, quanto segue:

- (i) il nome e i dettagli di contatto dell'entità Sodexo che agisce come Responsabile del trattamento e di ciascun titolare del trattamento per conto del quale l'entità Sodexo agisce, nonché del Data Protection Officer;
- (ii) le categorie di trattamento effettuate per conto di ciascun Titolare del trattamento;
- (iii) ove applicabile, i trasferimenti transfrontalieri di Dati personali verso un Paese terzo, compresa l'identificazione di tale Paese terzo e, nel caso di trasferimenti verso Paesi terzi non riconosciuti come Paesi adeguato, la documentazione di misure di salvaguardia adeguate;
- (iv) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'Articolo 32(1) del GDPR, al fine di garantire un livello di sicurezza adeguato al rischio, includendo tra l'altro, come appropriato:
  - a. la pseudonimizzazione e il criptaggio dei Dati personali;
  - b. la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
  - c. la possibilità di ripristinare la disponibilità dei Dati personali e l'accesso agli stessi in maniera tempestiva nell'eventualità di un incidente fisico o tecnico;
  - d. un processo per la verifica regolare, la valutazione dell'efficacia di misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Su richiesta, questi registri saranno divulgati alle Autorità di controllo competenti o al Titolare del trattamento.

Sodexo, in qualità di Responsabile del trattamento, mette a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare la conformità ai rispettivi obblighi e consente e contribuisce agli audit, comprese le indagini condotte dal Titolare del trattamento o da un altro soggetto incaricato da quest'ultimo. Inoltre, Sodexo informa immediatamente il Titolare del trattamento se, a suo parere, le istruzioni dovessero contravvenire al GDPR o a qualsiasi altra legge locale applicabile.

## NORMA 10 – RISPETTO DEI DIRITTI DEGLI INTERESSATI

### ***NORMA 10 – Sodexo assiste il Titolare del trattamento nel rispondere ai Diritti dell'Interessato.***

Sodexo e i suoi sub-responsabili (se presenti) attuano qualsiasi misura tecnica e organizzativa appropriata, nella misura in cui ciò sia possibile, quando viene richiesto da un Titolare del trattamento, per l'adempimento degli obblighi del Titolare del trattamento di rispondere alle richieste di esercizio dei diritti degli Interessati, incluso, nella misura legalmente consentita dalla legislazione SEE/UE, notificando tempestivamente il Titolare del trattamento in caso di ricezione di una richiesta da parte di un Interessato per accesso, rettifica, cancellazione, restrizione, portabilità, obiezione al Trattamento dei dati personali di tale persona.

Sodexo non risponde a tali richieste dell'Interessato senza il previo consenso scritto del Titolare del trattamento.

Sodexo fornisce al Titolare del trattamento cooperazione, assistenza e informazioni utili in relazione alla richiesta di un Interessato, al fine di aiutare il Titolare del trattamento ad adempiere al dovere di rispettare i diritti degli Interessati, nella misura consentita dalla legge e nella misura in cui il Titolare del trattamento non ha accesso a tali Dati personali attraverso il loro utilizzo per i servizi forniti da Sodexo o dai suoi sub-responsabili (se presenti).

Se Sodexo è stata incaricata dal Titolare del trattamento di fornire un indirizzo e-mail generico per consentire agli Interessati di esercitare i propri diritti, Sodexo potrebbe essere ulteriormente contattata direttamente dagli Interessati, a condizione che il Titolare del trattamento abbia fornito le informazioni pertinenti agli Interessati in conformità al GDPR.

L'Interessato ha il diritto di presentare un reclamo all'Autorità di controllo e di adire le vie legali in conformità con la Norma 17 della Processor Policy.

## NORMA 11 – RISPETTARE LE CONDIZIONI PER IL PROCESSO DECISIONALE INDIVIDUALE AUTOMATIZZATO E LA PROFILAZIONE E IMPLEMENTARE LE MISURE DI SALVAGUARDIA ADEGUATE

La Norma 11 non si applica ai Responsabili del trattamento.

## NORMA 12 – TRASPARENZA E INFORMAZIONE DELL'INTERESSATO

***NORMA 12 – Sodexo mette la Processor Policy a disposizione del Titolare del trattamento.***

La Processor Policy è messa a disposizione degli Interessati sul sito web ufficiale di Sodexo. Inoltre, la Politica globale sulla protezione dei dati (Appendice 5) include un calendario dedicato ai diritti dei beneficiari terzi.

La Processor Policy è disponibile e applicabile anche al Titolare del trattamento, in quanto sarà inclusa come riferimento negli accordi di trattamento dei dati stipulati con i Clienti o in qualsiasi altro documento vincolante. L'accordo di trattamento dei dati o qualsiasi altro documento vincolante stipulato con i Clienti contiene (i) l'impegno del Titolare del trattamento a far sì che, se il trasferimento riguarda categorie particolari di dati, l'Interessato sia stato informato o sarà informato prima del trasferimento della possibilità che i suoi dati siano trasmessi a un Paese terzo che non offre una protezione adeguata; (ii) l'impegno del Titolare del trattamento a informare l'Interessato dell'esistenza di responsabili del trattamento con sede al di fuori dell'UE e delle BCR; (iii) l'impegno del Titolare del trattamento a mettere a disposizione degli Interessati, su richiesta, una copia delle BCR e dell'accordo di trattamento dei dati o di qualsiasi altro documento vincolante.

## NORMA 13 – GARANTIRE UNA PROTEZIONE ADEGUATA PER I TRASFERIMENTI TRANSFRONTALIERI DI DATI PERSONALI

***NORMA 13 – Sodexo non trasferisce i Dati personali a terze parti al di fuori dell'UE/del SEE senza garantire un'adeguata protezione dei Dati personali trasferiti.***

Quando il trasferimento dei Dati personali viene effettuato a terze parti, l'entità Sodexo che trasferisce i Dati personali in qualità di Responsabile del trattamento:

- ottiene il consenso preventivo del Titolare del trattamento per tale trasferimento a terze parti;

- si assicura in un accordo di fornitura di servizi scritto, in un contratto o in qualsiasi altro documento vincolante, come un accordo di elaborazione dati, stipulato con la terza parte, che quest'ultima si impegni per iscritto a fornire garanzie sufficienti in conformità al GDPR e alle linee guida EDPB;
- sottoscrive il modulo 3 delle clausole contrattuali tipo della Commissione europea<sup>7</sup> (trasferimenti tra Responsabili del trattamento) e, se necessario, implementa misure supplementari in conformità a Schrems II.

## NORMA 14 – ADOTTARE LA PRIVACY FIN DALLA PROGETTAZIONE E DI DEFAULT

***NORMA 14 – Sodexo assiste il Titolare del trattamento nell'implementazione di misure tecniche e organizzative adeguate per rispettare i principi di protezione dei dati e facilitare la privacy fin dalla progettazione e di default.***

Sodexo assiste il Titolare del trattamento nell'implementazione di misure tecniche e organizzative adeguate per rispettare i principi di protezione dei dati e facilitare la privacy fin dalla progettazione e di default.

## NORMA 15 – ESECUZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

***NORMA 15 – Sodexo assiste il Titolare del trattamento nella conduzione delle Valutazioni d'impatto sulla protezione dei dati richieste.***

In conformità agli Articoli 35 e 36 e al Considerando 95 del GDPR, Sodexo fornisce una ragionevole assistenza, come stabilito nell'accordo per la fornitura di servizi, nel contratto o in qualsiasi altro documento vincolante con il Titolare del trattamento, per rendere disponibili le informazioni relative al Trattamento dei Dati personali che gestisce per conto del Titolare del trattamento, per garantire il rispetto da parte del Titolare del trattamento degli obblighi derivanti dall'esecuzione delle DPIA e dalla consultazione preventiva dell'autorità di controllo, ove necessario e su richiesta.

<sup>7</sup> Decisione di esecuzione (UE) 2021/914 della Commissione, del 4 giugno 2021, relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso Paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio

## Sezione B

### NORMA 16 – FORMAZIONE E SENSIBILIZZAZIONE

***NORMA 16 – Sodexo fornisce formazione ai dipendenti che hanno accesso permanente o regolare ai Dati personali e/o che sono coinvolti nella raccolta dei Dati personali o nello sviluppo di strumenti utilizzati per trattare i Dati personali per conto del Titolare del trattamento.***

#### Un programma di formazione completo

Affinché la Processor Policy sia applicabile ed efficace, il Global Data Protection Office ha implementato un programma di formazione completo che illustra i principi che regolano il Trattamento dei Dati personali ai sensi della presente Politica.

Un modulo generale è mirato a fornire materiale di formazione fondamentale sui principi di Protezione dei dati a tutti i dipendenti Sodexo, mentre i moduli specifici sono destinati ai dipendenti delle entità Sodexo che hanno accesso permanente o regolare ai Dati personali e/o sono coinvolti nella raccolta dei Dati personali o nella selezione o nello sviluppo degli strumenti utilizzati per trattare i Dati personali. Inoltre, i dipendenti di un'entità Sodexo devono essere informati circa i propri obblighi di rispettare le politiche di Protezione dei dati di Sodexo ai sensi del Codice di condotta per l'integrità aziendale di Sodexo<sup>8</sup>.

I moduli vengono aggiornati regolarmente per rispecchiare meglio le attività di Sodexo e far comprendere ai dipendenti come affrontare la protezione dei Dati personali nella propria quotidianità professionale.

Inoltre, gli Referenti unici locali per la protezione dei dati forniscono una formazione conforme alle leggi locali, tenendo conto dei relativi requisiti specifici.

#### Monitoraggio del programma di formazione

Le entità Sodexo adottano misure ragionevoli e appropriate per comunicare con i propri dipendenti e per fornire una formazione adeguata sui requisiti della Processor Policy.

Il completamento del programma di formazione sulla Protezione dei dati viene monitorato dai Referenti unici globali e locali per la protezione dei dati, insieme ai team di Apprendimento e Sviluppo globali e locali.

---

<sup>8</sup> Documento interno

## NORMA 17 – GESTIONE DEI DIRITTI DI PROTEZIONE DEI DATI

***NORMA 17 – Sodexo assiste il Titolare del trattamento a rispondere a una richiesta o a un reclamo ricevuto.***

Quando un Referente unico locale per la protezione dei dati riceve una richiesta da parte di un Interessato o un reclamo da parte dell'Autorità di controllo relativi a un Trattamento di Dati personali effettuato per conto di un Titolare del trattamento, è suo compito comunicarlo al Titolare del trattamento interessato senza ritardi ingiustificati (o entro il periodo di notifica concordato con il Titolare del trattamento) e senza obbligo di gestione (a meno che il Titolare del trattamento non abbia incaricato Sodexo in tal senso).

Il ruolo del Referente unico locale per la protezione dei dati è quello di gestire le richieste degli Interessati e i reclami delle Autorità di controllo solo su istruzione del Titolare del trattamento o qualora il Titolare del trattamento sia scomparso di fatto o abbia cessato di esistere giuridicamente o sia diventato insolvente.

Nel caso in cui il Titolare del trattamento sia scomparso di fatto o abbia cessato di esistere giuridicamente o sia diventato insolvente, Sodexo gestisce la richiesta senza indebito ritardo e in ogni caso entro un mese dal ricevimento della richiesta o, se necessario a causa della complessità e del numero delle richieste, entro il periodo di proroga di 3 mesi (1+2) massimo, dopo aver informato l'Interessato di tale proroga entro un mese dal ricevimento della richiesta, unitamente alle ragioni del ritardo, in conformità all'Articolo 12(3) del GDPR. In caso di richiesta effettuata per mezzo elettronico, le informazioni saranno fornite per mezzo elettronico, ove possibile, salvo diversa richiesta dell'interessato.

In tal caso, gli Interessati sono informati sulle fasi pratiche del sistema di gestione delle richieste e dei reclami nelle informative locali sulla protezione dei dati che implementano la Politica globale di gestione dei diritti per la protezione dei dati di cui all'Appendice 6.

## NORMA 18 – VALUTAZIONE DELLA COMPLIANCE: PROGRAMMA DI AUDIT

***NORMA 18 – Sodexo risponde alle richieste di audit dei Titolari del trattamento.***

Secondo il Programma globale di audit delle BCR di Sodexo, Sodexo verifica la conformità del Gruppo Sodexo alla Processor Policy e, in particolare, implementa un piano di audit che copre tutti gli aspetti della Processor Policy, compresi i metodi per garantire l'implementazione di azioni correttive.



Gli audit di Sodexo vengono effettuati annualmente dal team di Controllo Interno e anche dal team di Internal Audit del Gruppo, se necessario, su richiesta specifica del Group Data Protection Officer.

Gli auditor interni possono essere affiancati da auditor esterni laddove necessario.

I risultati di tutti gli audit devono essere comunicati al Group Data Protection Officer e ai Referenti unici locali per la protezione dei dati, nonché al Consiglio di Amministrazione del Gruppo Sodexo e ai membri competenti del Comitato esecutivo del Gruppo.

Le azioni correttive vengono decise sulla base del report prodotto.

Sodexo consente alle Autorità di controllo competenti di accedere ai risultati degli audit interni su richiesta e di effettuare un audit sulla Protezione dei dati di qualsiasi entità Sodexo, se necessario.

Sodexo risponde alle richieste di audit dei Titolari del trattamento secondo quanto stabilito negli accordi per la fornitura di servizi, nei contratti o in qualsiasi altro documento vincolante stipulato con i Titolari del trattamento.

Le entità Sodexo che agiscono in qualità di Responsabili del trattamento o i relativi sub-responsabili accettano, su richiesta scritta del Titolare del trattamento, di sottoporre le proprie strutture di trattamento dei dati a un audit delle attività di trattamento relative a tale Titolare. Detto audit può essere effettuato dal Titolare del trattamento o da un organismo di controllo composto da membri indipendenti e in possesso delle qualifiche professionali richieste, vincolati da un dovere di riservatezza, selezionati dal Titolare del trattamento, se del caso, in accordo con l'Autorità di controllo.

## NORMA 19 – MONITORAGGIO DELL'APPLICAZIONE DELLE BCR

### ***NORMA 19 – Sodexo monitora l'applicazione delle BCR.***

Il Global Data Protection Office ha istituito un registro dei rischi per garantire l'effettiva implementazione della Processor Policy.

Inoltre, ogni singolo Referente locale per la Protezione dei Dati riporta al Global Data Protection Office, con cadenza trimestrale, le best practice locali nell'implementazione della Processor Policy e le Valutazioni d'impatto sulla protezione dei dati effettuate a livello locale. I report dei Referenti per la protezione dei dati sono centralizzati e analizzati dal Global Data Protection Office. I risultati dell'analisi rientrano nella relazione annuale fornita al Comitato esecutivo di Sodexo.

## NORMA 20 – GLOBAL DATA PROTECTION OFFICE E RETE DEI REFERENTI UNICI LOCALI

***NORMA 20 – Sodexo garantisce la conformità alla Processor Policy attraverso una struttura di Governance della Protezione dei dati.***

Per supervisionare e garantire la conformità con la Processor Policy, Sodexo ha implementato, con il supporto del Comitato esecutivo di Sodexo, una struttura di Governance della Protezione dei dati come segue:

- un Group Data Protection Officer nominato in linea con l'Articolo 37 del GDPR che riferisce al Group General Counsel;
- un Global Data Protection Office composto da consulenti per la Protezione dei dati del Gruppo a livello globale, che supportano il Group Data Protection Officer nei suoi compiti;
- una rete di Referenti unici locali per la protezione dei dati (“DP SPoC locali”) a livello locale.

Il ruolo del Group Data Protection Officer è quello di monitorare la conformità a livello globale e di valutare l'efficacia del programma di Protezione dei dati di Sodexo (raccolta di informazioni per identificare le attività di trattamento, analisi e verifica della conformità, ecc.). Il Group Data Protection Officer fornisce alla Direzione consigli e raccomandazioni, nonché una relazione annuale sulle attività del Global Data Protection Office. Inoltre, il ruolo del Global Data Protection Office è quello di monitorare la conformità a livello globale e di valutare l'efficacia del Programma globale di compliance per la protezione dei dati di Sodexo.

Il Group Data Protection Officer consiglia e supporta i DP SPoC locali, quando necessario, al fine di conformarsi al Programma globale di protezione dei dati di Sodexo, di gestire le verifiche delle Autorità di controllo e di garantire che il ruolo del DP SPoC locale sia quello di gestire i reclami locali degli Interessati in conformità con la Norma 17, di riferire le principali questioni di Protezione dei dati al Group Data Protection Officer, di garantire la conformità a livello locale e di essere accessibile, nella lingua locale, agli Interessati locali, al Titolare del trattamento (un Cliente) e all'Autorità di controllo locale.

## NORMA 21 – DIRITTI DEI BENEFICIARI TERZI

***NORMA 21 – Sodexo conferisce espressamente dei diritti agli Interessati sia quando tali diritti sono direttamente opponibili a Sodexo, sia quando i diritti sono opponibili a Sodexo nel caso in cui l'Interessato non sia in grado di presentare un reclamo contro il Titolare del trattamento.***

### **1. Diritti che sono direttamente opponibili a Sodexo in qualità di Responsabile del trattamento:**

Gli Interessati possono far valere la Processor Policy nei confronti delle entità Sodexo che agiscono in qualità di Responsabili del trattamento, in particolare:

- **obbligo di rispettare le istruzioni del Titolare del trattamento in merito al Trattamento dei Dati personali, compreso il trasferimento dei Dati personali in Paesi terzi;**
- **obbligo di implementare misure di sicurezza tecniche e organizzative adeguate e obbligo di comunicare qualsiasi Violazione dei Dati personali al Titolare del trattamento (Norma 7);**
- **obbligo di rispettare le condizioni di ingaggio di un sub-responsabile interno o esterno al Gruppo (Norma 7);**
- **obbligo di cooperare con il Titolare del trattamento e di assisterlo nell'adempimento e nella dimostrazione della conformità alla legge, ad esempio per rispondere alle richieste degli Interessati in relazione ai propri diritti (Norme 1B, 2A, 5, 10, 17 e 23);**
- **trasparenza in merito alla Processor Policy:** gli Interessati hanno facile accesso ai propri diritti di beneficiari terzi, in quanto la Processor Policy è disponibile sull'Intranet e sul sito web ufficiale di Sodexo. Su richiesta possono ottenere una copia della presente politica dai membri delle BCR che agiscono in qualità di Responsabili del trattamento. Inoltre, la Politica globale sulla protezione dei dati (Appendice 5) include un calendario dedicato ai diritti dei beneficiari terzi;
- **trasparenza sui casi in cui la legislazione nazionale impedisce al Gruppo Sodexo di essere conforme alle BCR:** possono far valere la Norma 23;
- **diritto di reclamo:** quando un Referente unico locale per la protezione dei dati riceve un reclamo da un Interessato in merito al Trattamento dei Dati personali effettuato per conto di un Titolare del trattamento, lo comunicherà tempestivamente al Titolare del trattamento interessato, senza obbligo di gestione. Il Referente unico locale per la protezione dei dati gestisce i reclami di tale Interessato solo su istruzione del Titolare del trattamento o se il Titolare del trattamento è scomparso di fatto o ha cessato di esistere giuridicamente o è

diventato insolvente. In tal caso, gli Interessati ricevono informazioni sulle fasi pratiche del sistema di reclamo nelle politiche locali di protezione dei dati che attuano la Politica globale di gestione dei diritti di protezione dei dati di cui all'Appendice 6. Gli Interessati sono informati circa: (i) dove presentare il reclamo; (ii) in quale forma; (iii) i tempi di risposta al reclamo; (iv) le conseguenze in caso di rifiuto del reclamo; (v) le conseguenze nel caso in cui il reclamo sia considerato giustificato; (vi) il diritto di presentare un reclamo presso il Tribunale o l'Autorità di controllo competente;

- **cooperazione:** gli Interessati possono far valere la Norma 24;
- **responsabilità:** Sodexo SA, in qualità di sede centrale europea di Sodexo che agisce in veste di Responsabile del trattamento, si assume la responsabilità e si impegna a intraprendere le azioni necessarie per porre rimedio agli atti di altre entità Sodexo con sede al di fuori dell'UE/del SEE o alle violazioni causate da un sub-responsabile esterno con sede al di fuori dell'UE/del SEE, a risarcire eventuali danni derivanti da una violazione delle BCR o a dimostrare che tali entità Sodexo con sede al di fuori dell'UE/del SEE non sono responsabili della violazione o che le violazioni causate da un sub-responsabile esterno non hanno avuto luogo. La suddetta Sodexo SA che ha accettato la responsabilità avrà l'onere della prova per dimostrare che l'entità Sodexo al di fuori dell'UE/del SEE non è responsabile di alcuna violazione delle norme che ha portato l'Interessato a richiedere il risarcimento dei danni. Qualora riesca a dimostrare che la suddetta entità Sodexo non è responsabile dell'evento che ha causato il danno, potrà esonerarsi da qualsiasi responsabilità.

## 2. Diritti opponibili a Sodexo in qualità di Responsabile del trattamento, nel caso in cui l'Interessato non sia in grado di presentare un reclamo nei confronti del Titolare del trattamento:

Gli Interessati che rientrano nell'ambito di applicazione della Processor Policy sono beneficiari terzi in virtù della presente Norma del beneficiario terzo all'interno della Processor Policy, a cui viene conferito un effetto vincolante dall'accordo infragruppo firmato tra le entità del Gruppo Sodexo.

Per essere applicata dal Titolare del trattamento, la Processor Policy sarà inclusa nell'accordo per la fornitura di servizi, nel contratto o in qualsiasi altro documento vincolante firmato tra un'entità Sodexo che agisce per conto di un Titolare del trattamento e tale Titolare (un Cliente).

Gli Interessati hanno il diritto di far rispettare la Processor Policy al Titolare del trattamento per conto del quale i Dati personali sono trattati da Sodexo, presentando un reclamo all'Autorità di controllo competente o ad un tribunale competente per il Titolare dell'UE/del SEE.

Tuttavia, gli Interessati possono far valere le Norme stabilite nella Processor Policy in qualità di beneficiari terzi, qualora non siano in grado di presentare un ricorso contro il Titolare del trattamento in relazione alla violazione di uno qualsiasi degli impegni della Processor Policy da parte di un'entità di Sodexo (o di un sub-responsabile) che agisce in qualità di Responsabile del trattamento (ad esempio, nel caso in cui il Titolare del trattamento sia di fatto scomparso o abbia cessato di esistere giuridicamente o sia divenuto insolvente, a meno che un'entità subentrante non abbia assunto la totalità degli obblighi giuridici del Titolare del trattamento per contratto o per

effetto di legge, nel qual caso gli Interessati possono far valere i loro diritti nei confronti di tale entità).

In tal caso, gli Interessati possono almeno far valere le seguenti norme contenute nella Processor Policy:

- obbligo di rispettare le BCR (Norma 1);
- diritti dei beneficiari terzi (Norma 21);
- la responsabilità e l'onere della prova spettano a Sodexo e non all'Interessato (Norma 22);
- facile accesso alle BCR e trasparenza (Norma 12);
- gestione dei reclami (Norma 17);
- cooperazione con le Autorità di controllo (Norma 24);
- trasferimenti dei Dati personali (Norma 13);
- elenco delle entità vincolate dalle BCR;
- obbligo di cooperare con il Titolare del trattamento (Norma 1);
- trasparenza, correttezza e liceità (Norma 2);
- limitazione della finalità (Norma 3);
- qualità dei dati (Norme 4, 5 e 6);
- sicurezza (Norma 7);
- diritti dell'Interessato (Norma 10);
- sub-trattamento (Norma 7B);
- trasparenza sui casi in cui la legislazione nazionale impedisce al gruppo di essere conforme alle BCR (Norma 23).

### **3. Disposizioni in materia di risarcimento e giurisdizione (per entrambi i diritti dell'Interessato di cui ai punti 1. e 2.)**

Gli Interessati possono presentare un reclamo (i) all'Autorità di controllo francese (la “*Commission Nationale de l'Informatique et des Libertés*”, la “CNIL”) contro Sodexo SA responsabile dell'esportazione dei dati (a) all'Autorità di controllo nello Stato membro di residenza abituale, (b) del luogo di lavoro o (c) del luogo della presunta violazione e ii) ai tribunali francesi competenti dove Sodexo SA ha la propria sede o ai tribunali competenti degli Stati membri dell'UE/del SEE dove risiedono gli Interessati stessi. Qualora Sodexo, in qualità di Responsabile del trattamento, e il Titolare del trattamento coinvolto nello stesso trattamento di Dati personali siano ritenuti responsabili di qualsiasi danno causato da tale trattamento, gli Interessati hanno il diritto di ricevere un risarcimento per l'intero danno direttamente da Sodexo in qualità di Responsabile del trattamento.

## NORMA 22 – RESPONSABILITÀ

### ***NORMA 22 – Sodexo rispetta le seguenti norme in materia di responsabilità.***

Qualora un Interessato subisca un danno a causa del Trattamento dei dati personali da parte di Sodexo in violazione della Processor Policy, il Titolare del trattamento mantiene la responsabilità di essere conforme al GDPR. I Titolari del trattamento che rientrano nell'ambito del GDPR trasmetteranno a Sodexo alcuni obblighi di Protezione dei dati negli accordi per la fornitura di servizi, nei contratti o in altri documenti vincolanti che Sodexo ha stipulato con essi. Di conseguenza, se Sodexo non rispetta le istruzioni del Titolare del trattamento in merito al Trattamento dei Dati Personali, come stabilito nell'accordo per la fornitura di servizi, nel contratto o in altri documenti vincolanti che stipula con un Titolare del trattamento, il Titolare del trattamento potrebbe violare il GDPR e il contratto e Sodexo potrebbe subire una richiesta di risarcimento per violazione del contratto, che potrebbe comportare il pagamento di un indennizzo per eventuali danni materiali o morali e di disagio o altri rimedi giudiziari.

In tali casi, se un Titolare del trattamento dimostra di aver subito un danno e che è probabile che questo si sia verificato a causa di una violazione della Processor Policy da parte di un'entità Sodexo al di fuori dell'Europa (o di un sub-responsabile terzo con sede al di fuori dell'Europa), tale Titolare del trattamento ha il diritto di far valere la Processor Policy nei confronti di Sodexo SA, in quanto sede centrale di Sodexo nell'UE.

Sodexo SA si assume la responsabilità e si impegna a intraprendere le azioni necessarie per porre rimedio agli atti di altre entità Sodexo con sede al di fuori dell'UE/del SEE o alle violazioni causate da un sub-responsabile esterno con sede al di fuori dell'UE/del SEE, a risarcire eventuali danni derivanti da una violazione delle BCR o a dimostrare che tali entità Sodexo con sede al di fuori dell'UE/del SEE non sono responsabili della violazione o che le violazioni causate da un sub-responsabile esterno non hanno avuto luogo. Inoltre, Sodexo SA avrà l'onere della prova per dimostrare che l'entità Sodexo al di fuori dell'UE/del SEE non è responsabile di alcuna violazione delle norme che ha portato l'Interessato a richiedere i danni. Qualora riesca a dimostrare che la suddetta entità Sodexo non è responsabile dell'evento che ha causato il danno, potrà esonerarsi da qualsiasi responsabilità.

# 03

## Disposizioni finali



## **NORMA 23 – AZIONI IN CASO DI LEGISLAZIONE O PRASSI NAZIONALI CHE IMPEDISCAO IL RISPETTO DELLE BCR – RICHIESTA GIURIDICAMENTE VINCOLANTE DI DIVULGAZIONE DEI DATI PERSONALI**

***NORMA 23.A – Sodexo effettua una valutazione delle leggi e delle prassi locali applicabili prima di qualsiasi trasferimento di Dati personali, per garantire che non le impediscano di adempiere ai suoi obblighi ai sensi della Processor Policy e che non abbiano un effetto sostanziale sulla sua capacità di rispettare la presente politica.***

***NORMA 23.B – Sodexo provvede a informare tempestivamente il Titolare del trattamento e/o Sodexo SA o il membro delle BCR dell'UE/del SEE o il Group Data Protection Officer e qualsiasi altro Referente unico locale per la protezione dei dati, nonché l'entità Sodexo che agisce in qualità di Esportatore dei dati, qualora abbia motivo di ritenere che la legge o le prassi locali applicabili le impediscano di adempiere agli obblighi previsti dalla Processor Policy e abbiano un effetto sostanziale sulla sua capacità di rispettare la presente Processor Policy.***

***NORMA 23.C – In caso di ricezione di una richiesta legalmente vincolante di divulgazione di Dati personali soggetti alla Processor Policy, Sodexo si impegna a informare tempestivamente Sodexo SA, il Group Data Protection Officer, l'entità Sodexo che agisce in qualità di Esportatore dei dati, il Titolare del trattamento (tramite l'entità Sodexo che agisce in qualità di Esportatore dei dati) e, ove possibile, l'interessato se istruito dal Titolare del trattamento, a meno che ciò non sia proibito da un'autorità preposta all'applicazione della legge; inoltre, mette la richiesta in attesa, a meno che ciò non sia proibito da un'autorità o un'agenzia preposta all'applicazione della legge. La notifica includerà, tra l'altro, informazioni sui dati richiesti, il numero di richieste, l'ente richiedente e la base giuridica per la divulgazione.***

### **Valutazione della legge e delle prassi locali applicabili**

In conformità alle raccomandazioni dell'EDPB<sup>9</sup> e alle Clausole contrattuali tipo dell'Unione europea<sup>10</sup>:

Le entità Sodexo garantiscono di non avere motivo di ritenere che le leggi e le prassi locali applicabili impediscano loro di adempiere agli obblighi previsti dalla Processor Policy o agli obblighi contrattuali con il Titolare del trattamento e abbiano un effetto sostanziale sulla loro capacità di rispettare la presente politica o i propri obblighi. Ciò si basa sulla consapevolezza che le leggi e le prassi locali applicabili che rispettano l'essenza dei diritti e delle libertà fondamentali e non vanno oltre quanto necessario e proporzionato in una società democratica per

<sup>9</sup> Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei Dati personali dell'UE adottate il 18 giugno 2021.

<sup>10</sup> Decisione di esecuzione (UE) 2021/914 della Commissione, del 4 giugno 2021, relativa alle clausole contrattuali tipo per il trasferimento di Dati personali verso Paesi terzi a norma del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio.



salvaguardare uno degli obiettivi elencati nell'Articolo 23(1) del GDPR non sono in contraddizione con la Processor Policy.

Sodexo dichiara che nel fornire questa garanzia ha tenuto in debito conto, con l'ausilio del Group Data Protection Officer, in particolare dei seguenti elementi:

- le circostanze specifiche del trasferimento, ivi inclusi la lunghezza della catena di trattamento, il numero di attori coinvolti e i canali di trasmissione utilizzati; i trasferimenti successivi previsti; il tipo di destinatario; la finalità del trattamento; le categorie e il formato dei Dati personali trasferiti; il settore economico in cui avviene il trasferimento; il luogo di conservazione dei dati trasferiti;
- le leggi e le prassi della legislazione locale applicabile – comprese quelle che richiedono la divulgazione dei dati alle autorità pubbliche o che ne autorizzano l'accesso da parte di tali autorità – rilevanti alla luce delle circostanze specifiche del trasferimento, delle limitazioni e delle misure di salvaguardia applicabili, nonché dell'applicabilità dei diritti degli interessati e dell'efficacia dei rimedi legali per questi ultimi;
- qualsiasi misura di salvaguardia contrattuale, tecnica o organizzativa pertinente messa in atto per integrare le misure di salvaguardia ai sensi della Processor Policy e secondo le istruzioni del Titolare del trattamento, comprese le misure applicate durante la trasmissione e il trattamento dei Dati personali nelle entità Sodexo.

Le entità Sodexo si impegnano a documentare questa valutazione e a renderla disponibile al Titolare del trattamento e all'autorità di controllo competente su richiesta.

Qualora un'entità Sodexo abbia motivo di ritenere che la legge e/o le prassi locali applicabili o una richiesta di divulgazione possano impedirle di adempiere ai propri obblighi ai sensi della Processor Policy o ai propri obblighi contrattuali con il Titolare del trattamento e che abbiano un effetto sostanziale sulla sua capacità di rispettare la presente Processor Policy o i propri obblighi contrattuali con il Titolare del trattamento, informerà tempestivamente, in conformità all'accordo per la fornitura di servizi, al contratto o a qualsiasi altro documento vincolante concluso con il Titolare del trattamento (un Cliente):

- l'entità Sodexo che agisce in qualità di Esportatore dei dati, la quale inoltrerà la notifica al Titolare del trattamento, che ha il diritto di sospendere il trasferimento dei Dati personali e/o di risolvere il contratto o altro documento vincolante con Sodexo; e
- Sodexo SA; o
- il Group Data Protection Officer e qualsiasi altro Referente unico locale per la protezione dei dati.

A seguito di questa notifica Sodexo SA, insieme all'entità Sodexo che agisce in qualità di Esportatore dei dati, con l'assistenza del Group Data Protection Officer e, se necessario, del Referente unico locale per la protezione dei dati e, se del caso, in consultazione con il Titolare del trattamento, identificherà tempestivamente le misure appropriate (ad esempio, misure

tecniche o organizzative per garantire la sicurezza e la riservatezza) da adottare per affrontare la situazione.

Sodexo sospenderà il trasferimento dei dati qualora ritenga che non possano essere garantite misure di salvaguardia adeguate per tale trasferimento, o qualora riceva istruzioni in tal senso dal Titolare del trattamento o dall'Autorità di controllo competente. In questo caso, l'entità Sodexo situata al di fuori dell'UE/del SEE che ritiene di essere o di essere diventata soggetta a leggi o prassi non in linea con i requisiti della Processor Policy non farà parte delle BCR-Processor.

### **Richiesta di Divulgazione dei Dati personali da parte di un'autorità incaricata dell'applicazione della legge o di un organo di sicurezza statale**

In caso di richiesta legalmente vincolante di divulgazione dei Dati personali o di accesso diretto ai Dati personali da parte di un'autorità incaricata dell'applicazione della legge o di un organismo di sicurezza statale, le entità Sodexo che la ricevono o ne vengono a conoscenza ne daranno tempestivamente comunicazione a Sodexo SA, al Group Data Protection Officer e all'entità Sodexo che agisce come Esportatore dei dati.

L'entità Sodexo che agisce come Esportatore dei dati inoltrerà la notifica al Titolare del trattamento e, ove possibile, all'interessato se istruito dal Titolare del trattamento.

Sodexo valuta caso per caso ogni richiesta di accesso ai dati da parte di un'autorità incaricata dell'applicazione della legge o di un ente di sicurezza statale. Sodexo si adopera al meglio per informare l'autorità richiedente interessata sugli obblighi di Sodexo ai sensi del GDPR e per ottenere il diritto di rinunciare a questo divieto.

Sodexo mette in attesa tale richiesta per un ragionevole periodo di tempo, al fine di informare gli stakeholder sopra citati per la presente Processor Policy prima di divulgare i dati all'autorità richiedente. Sodexo informa chiaramente gli stakeholder di cui sopra in merito alla richiesta, comprese, a titolo esemplificativo ma non esaustivo, le informazioni sui dati richiesti, il numero di richieste, l'autorità richiedente interessata e la base giuridica per la divulgazione.

Qualora, in casi specifici, la sospensione e/o la notifica siano vietate, Sodexo farà del suo meglio per ottenere il diritto di esenzione da tale divieto, al fine di comunicare il maggior numero di informazioni possibili e il più tempestivamente possibile ed essere in grado di dimostrarlo, documentando i migliori sforzi compiuti.

Qualora, nonostante l'impegno profuso, Sodexo non sia in grado di informare i suddetti stakeholder e di sospendere la richiesta, fornisce informazioni generali sulle richieste ricevute ai suddetti stakeholder (ad esempio, numero di richieste di divulgazione, tipo di dati richiesti, autorità richiedente, se possibile), nella misura in cui la suddetta autorità richiedente l'abbia autorizzata a divulgare tali informazioni a terze parti. L'entità Sodexo che agisce come Esportatore dei dati trasmetterà queste informazioni al Titolare del trattamento.

In ogni caso, i trasferimenti di Dati personali a qualsiasi autorità pubblica non possono essere massicci, sproporzionati e indiscriminati in modo tale da andare oltre quanto necessario in una società democratica.

## Trasferimenti o divulgazioni transfrontalieri di dati non autorizzati dal diritto dell'Unione

Per le entità Sodexo con sede nel SEE, qualsiasi sentenza di un tribunale o di un organo giurisdizionale e qualsiasi decisione di un'autorità amministrativa di un Paese terzo che richieda a un Titolare del trattamento o a un Responsabile del trattamento di trasferire o divulgare i Dati personali può essere riconosciuta o applicata in qualsiasi modo solo se basata su un accordo internazionale, come un trattato di mutua assistenza giudiziaria, in vigore tra il Paese terzo richiedente e l'Unione o uno Stato membro, fatti salvi gli altri motivi di trasferimento ai sensi del Capitolo V del GDPR.

Qualsiasi entità Sodexo che riceva tale richiesta informerà tempestivamente, in conformità all'accordo per la fornitura di servizi, al contratto o a qualsiasi altro documento vincolante concluso con il Titolare del trattamento (un Cliente):

- l'entità Sodexo che agisce in qualità di Esportatore dei dati, la quale inoltrerà la notifica al Titolare del trattamento, che ha il diritto di sospendere il trasferimento dei Dati personali e/o di risolvere il contratto o altro documento vincolante con Sodexo; e
- Sodexo SA; o
- il Group Data Protection Officer e qualsiasi altro Referente unico locale per la protezione dei dati.

## NORMA 24 – COOPERAZIONE CON LE AUTORITÀ DI CONTROLLO

***NORMA 24 – Sodexo assiste il Titolare del trattamento nell'adempimento del suo obbligo di cooperazione con le Autorità di controllo e in conformità alla Procedura di cooperazione delle BCR.***

Ai sensi della Processor Policy, le entità Sodexo assistono il Titolare del trattamento nell'adempimento del suo obbligo di cooperazione con le Autorità di controllo e in conformità alla Procedura di cooperazione delle BCR di cui all'Appendice 3 e, in particolare, collaborano con le Autorità di controllo e accettano di essere controllate da queste ultime e di conformarsi al parere di tali Autorità di controllo competenti per qualsiasi questione relativa a tali BCR.

## NORMA 25 – AGGIORNAMENTO DELLE BCR

### ***NORMA 25 – Sodexo rispetta la Procedura di aggiornamento delle BCR.***

Ai sensi della Procedura di aggiornamento delle BCR riportata nell'Appendice 4, Sodexo segnala una volta all'anno qualsiasi modifica amministrativa alla Processor Policy o all'elenco delle entità Sodexo aderenti alle BCR alle Autorità di controllo pertinenti, tramite l'Autorità di controllo competente (ossia la CNIL), con una breve spiegazione delle ragioni a sostegno dell'aggiornamento.

In caso di modifiche sostanziali tali da influire sul livello di protezione offerto dalle BCR o da influire in modo significativo sulle stesse (ad esempio, modifiche al carattere vincolante), queste vengono comunicate tempestivamente alle Autorità di controllo pertinenti, tramite l'Autorità di controllo competente (ad esempio, la CNIL).

Qualsiasi modifica alle BCR viene notificata ai dipendenti attraverso l'Intranet di Sodexo e agli altri Interessati e Titolari del trattamento sul sito web ufficiale di Sodexo.

In caso di modifiche sostanziali alle BCR, Sodexo informa anche il Titolare del trattamento di qualsiasi cambiamento che possa influire sulle attività di trattamento concordate contrattualmente. Il Titolare del trattamento ha la possibilità di opporsi a tale modifica o di risolvere l'accordo per la fornitura di servizi, il contratto o qualsiasi altro documento vincolante. Il Group Data Protection Officer, con il supporto del team legale del Gruppo, tiene un elenco completamente aggiornato delle entità Sodexo aderenti alle BCR, tiene traccia e registra qualsiasi aggiornamento delle BCR e fornisce le informazioni necessarie al Titolare del trattamento.

Sodexo si accerta che non venga effettuato alcun trasferimento a una nuova entità Sodexo fintanto che questa non sia effettivamente vincolata dalle BCR o da altre salvaguardie appropriate e non sia in grado di garantire la conformità.

## NORMA 26 – VINCOLATIVITÀ DELLE BCR

### ***NORMA 26 – Tutte le entità Sodexo facenti parte del Gruppo Sodexo che agiscono in qualità di Responsabile del trattamento rispettano la Processor Policy, compresi i loro dipendenti.***

Quando agiscono come Responsabile del trattamento, le entità Sodexo che hanno aderito alla Processor Policy forniscono quest'ultima al Titolare del trattamento come parte dell'accordo per la fornitura di servizi, del contratto o di qualsiasi altro documento vincolante con il Titolare.

Quando le entità Sodexo in qualità di Responsabile del trattamento subappaltano i loro obblighi con il previo consenso del Titolare del trattamento, lo fanno solo tramite un accordo scritto con il sub-responsabile.

Quando un membro delle BCR non appartenente al SEE cessa di far parte del Gruppo Sodexo o di essere vincolato dalle BCR, tale entità Sodexo continua ad applicare i requisiti delle BCR al trattamento dei Dati personali che le sono stati trasferiti tramite le BCR, a meno che, al momento di lasciare il Gruppo Sodexo o di cessare di essere vincolato dalle BCR, tale membro non cancelli, renda anonimi o restituisca l'intero ammontare di questi Dati personali a un'entità Sodexo a cui si applicano ancora le BCR.

La Processor Policy è stata condivisa con tutti i dipendenti come nuova politica di Protezione dei dati del Gruppo ed è disponibile in qualsiasi momento sull'Intranet ufficiale di Sodexo e sul sito web ufficiale.

Tutti i dipendenti Sodexo sono tenuti a garantire la riservatezza e a rispettare le politiche di protezione dei dati, come stabilito nella clausola di protezione dei dati inclusa nel proprio contratto di lavoro. In caso di inosservanza di tali politiche di protezione dei dati è possibile applicare adeguate sanzioni disciplinari o azioni giudiziarie in conformità alla legge.

# 04

## Appendici



- Appendice 1: Definizioni
- Appendice 2: Politica globale di raccolta e conservazione dei dati (Responsabile del trattamento)
- Appendice 3: Procedura di cooperazione delle BCR
- Appendice 4: Procedura di aggiornamento delle BCR
- Appendice 5: Politica globale sulla protezione dei dati di Sodexo
- Appendice 6: Politica globale di gestione dei diritti per la protezione dei dati
- Appendice 7: Descrizione dell'ambito di applicazione materiale della Processor Policy

## Appendice 1 – Definizioni

Quando l'oggetto del presente documento riguarda i Dati personali, i termini e le espressioni senza iniziale maiuscola utilizzati (ad esempio "Dati personali", "trattamento", ecc.) saranno interpretati in conformità al significato loro attribuito nel GDPR. Inoltre, i termini con iniziale maiuscola indicati nel presente documento avranno, ai fini delle presenti BCR, il significato loro assegnato di seguito.

- Per **Paese adeguato** si intende un Paese che assicura un livello di protezione adeguato in base a una "decisione di adeguatezza" adottata dalla Commissione europea, la quale ha il potere di determinare se un Paese terzo assicura un livello di protezione adeguato per i Dati personali in virtù della relativa normativa nazionale o degli impegni internazionali sottoscritti.
- Per **Cliente** si intendono organizzazioni o società esterne, con sede nell'UE o nel SEE, che chiedono al Gruppo Sodexo di eseguire servizi per loro conto per i loro dipendenti in loco che sono gli utenti finali di questi servizi, in qualità di Titolare del trattamento.
- Per **Titolare del trattamento** si intende il soggetto che determina le finalità e i mezzi del trattamento dei Dati personali.
- Per **Esportatore dei dati** si intende un Titolare del trattamento (o, ove consentito, un Responsabile del trattamento) situato nell'UE che trasferisce i Dati personali a un Importatore dei dati.
- Per **Importatore di dati** si intende un Titolare o un Responsabile del trattamento situato in un Paese terzo che riceve i Dati personali dall'Esportatore dei dati.
- Per **Interessato** si intende una persona fisica identificata o identificabile i cui Dati personali sono oggetto di trattamento all'interno del Gruppo Sodexo, compresi i Dati personali di candidati, dipendenti, clienti, consumatori/beneficiari, fornitori/venditori, appaltatori/subappaltatori o terze parti di Sodexo, sia attuali che passati e potenziali.
- Per **EDPB** si intende il Comitato europeo per la protezione dei dati (*European Data Protection Board*). Si tratta di un organo indipendente europeo che contribuisce alla costante applicazione delle norme sulla protezione dei dati in tutta l'Unione europea, oltre a promuovere la cooperazione tra le autorità europee che si occupano di protezione dei dati.
- Per **UE** si intende l'Unione europea.
- Per **SEE** si intende lo Spazio Economico Europeo.
- Per **Regolamento Generale sulla Protezione dei Dati o GDPR** si intende il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 sulla protezione delle



persone fisiche in materia di trattamento di Dati personali e libera circolazione di tali dati e abrogativo della Direttiva 95/46/CE.

- Per **Group Data Protection Officer** si intende la persona nominata con l'approvazione del Comitato esecutivo del Gruppo Sodexo per supervisionare le questioni relative alla riservatezza dei dati a livello di Gruppo Sodexo, per definire e diffondere il programma di conformità alla protezione dei dati di Sodexo e le best practice relative alla riservatezza dei dati e per garantirne l'attuazione, come stabilito dalla Norma 20.
- Per **Referente unico locale per la protezione dei dati** si intende la persona nominata da un'entità Sodexo, incaricata di gestire le questioni relative alla privacy dei dati a livello locale. In alcuni casi, il Referente unico locale per la protezione dei dati può essere nominato come Local Data Protection Officer, se richiesto dalla legge sulla protezione dei dati.
- Per **Dati personali** si intende qualunque tipo di informazione relativa a una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- Per **Violazione dei Dati personali** si intende qualunque violazione della sicurezza che porta alla distruzione accidentale o illegale, perdita, alterazione o divulgazione non autorizzata di, o accesso a, Dati Personali trasmessi, archiviati o altrimenti trattati.
- Per **Trattamento o Trattamento dei Dati personali** si intende 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.
- Per **Responsabile del trattamento** si intende la persona fisica o giuridica, l'agenzia o qualsiasi altro organismo che tratta i Dati personali per conto del Titolare del trattamento.
- Per **Dati personali sensibili** designati come “Categorie particolari di dati” ai sensi del GDPR si intende qualsiasi Dato personale che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale e il trattamento di dati genetici, dati biometrici al fine di identificare in modo univoco una persona fisica, dati relativi alla salute o dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica. Questa definizione include anche i Dati personali relativi a condanne penali e reati.
- Per **Programma globale di protezione dei dati Sodexo** si intende il programma presentato e convalidato dal Group Data Protection Officer al Comitato esecutivo del Gruppo Sodexo.
- Per **Gruppo Sodexo o entità Sodexo o membri della Processor Policy** si intende qualsiasi società o interesse economico che sia direttamente o indirettamente di proprietà di Sodexo

con almeno il 50% del capitale sociale e degli aventi diritto di voto e che sia vincolato alle Norme vincolanti d'impresa Sodexo.

- Per **Autorità di controllo** si intende un'autorità pubblica indipendente istituita da uno Stato membro come specificato nel GDPR.

## Appendice 2 – Politica globale di raccolta e conservazione dei dati (Responsabile del trattamento)

### INTRODUZIONE

Sodexo si impegna a proteggere la privacy dei propri dipendenti, clienti, consumatori e qualsiasi altro individuo e ha implementato solide politiche, programmi e pratiche in materia di privacy. In particolare, quando Sodexo, in qualità di Responsabile del trattamento, effettua un Trattamento di dati personali secondo le istruzioni documentate di un Titolare del trattamento.

Al fine di soddisfare le best practice in materia di conservazione dei Dati personali, Sodexo ha adottato una Politica globale di conservazione dei dati. La presente Politica descrive il modo in cui Sodexo, quando agisce in qualità di Responsabile del trattamento, si attiene ai principi del GDPR e di ogni altra legge applicabile e, quindi, come Sodexo assicura la tutela dei diritti e delle libertà delle persone.

### DEFINIZIONI

- Per **Titolare del trattamento** si intende la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o congiuntamente ad altri, determina le finalità e i mezzi del trattamento dei Dati personali. Nella presente politica, per Titolare del trattamento si intende un Cliente.
- Per **Interessato** si intende una persona fisica identificata o identificabile i cui Dati personali sono oggetto di trattamento all'interno di Sodexo, compresi i Dati personali di candidati, dipendenti, clienti, consumatori/beneficiari, fornitori/venditori, appaltatori/subappaltatori o terze parti di Sodexo, sia attuali che passati e potenziali.
- Per **Regolamento Generale sulla Protezione dei Dati o GDPR** si intende il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 sulla protezione delle persone fisiche in materia di trattamento di Dati personali e libera circolazione di tali dati e abrogativo della Direttiva 95/46/CE.
- Per **Dati personali** si intende qualunque tipo di informazione relativa a una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- Per **Trattamento dei dati personali** si intende qualsiasi operazione o insieme di operazioni eseguite sui Dati personali o su insiemi di Dati personali, con o senza l'ausilio di mezzi

automatizzati, quali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione o messa a disposizione in altro modo, l'allineamento o la combinazione, la limitazione, la cancellazione o la distruzione.

- Per **entità Sodexo** si intende qualsiasi società, partnership o altra entità o organizzazione ammessa di volta in volta come membro del Gruppo Sodexo.

## **COME ASSISTERE IL TITOLARE DEL TRATTAMENTO NELL'ADEMPIMENTO DELL'OBBLIGO DI LIMITAZIONE DELLA CONSERVAZIONE**

- a. Rispettare le istruzioni del Titolare del trattamento in merito al periodo di conservazione dei Dati personali.

Il Responsabile del trattamento deve sempre attenersi alle istruzioni del Titolare del trattamento durante il Trattamento dei Dati personali. Ciò vale anche per la cancellazione dei Dati personali al termine del ciclo di vita del Trattamento.

I Dati personali saranno pertanto sempre conservati e/o cancellati e/o anonimizzati secondo le istruzioni del Titolare del trattamento in ottemperanza del periodo di conservazione fissato da quest'ultimo, a condizione che tali istruzioni non siano in conflitto con la normativa locale applicabile.

Pertanto se, durante l'esecuzione del contratto, il Titolare del trattamento istruisce ulteriormente Sodexo a cancellare o restituire alcuni dei Dati personali trattati, Sodexo dovrà conformarsi a tale richiesta (a condizione che tale istruzione non sia in conflitto con la normativa locale applicabile).

Sodexo eliminerà i Dati personali solo in modo sicuro, in conformità con la Politica di sicurezza e informazione del Gruppo.

- b. Risoluzione del contratto

Sodexo e i suoi eventuali sub-responsabili chiederanno al Titolare del trattamento di determinare la propria scelta in merito alla cancellazione, alla restituzione o all'anonimizzazione dei Dati personali. La scelta sarà specificata nel contratto o in un altro documento vincolante sottoscritto con il Titolare del trattamento.

Al termine della fornitura dei servizi relativi al Trattamento dei dati personali, Sodexo in qualità di Responsabile del trattamento e i suoi eventuali sub-responsabili, agirà in ottemperanza della scelta del Titolare del trattamento esplicitata nel contratto ed eliminerà, anonimizzerà tutti i Dati personali trasferiti o restituirà le relative copie al Titolare del trattamento. Provvederà poi a dimostrare quanto fatto fornendo un'attestazione al Titolare del trattamento. L'attestazione deve contenere almeno la data della cancellazione o dell'anonimizzazione, l'elenco dei Dati personali cancellati o resi anonimi e la firma del titolare dell'azienda interessata e del Data Protection Officer o del Referente unico locale per la protezione dei dati. Se la normativa locale applicabile stabilisce un periodo obbligatorio di conservazione dei Dati personali e richiede che Sodexo conservi i dati

personali di conseguenza, Sodexo assicura che garantirà la riservatezza dei Dati personali e non tratterà più attivamente i Dati personali se non per la finalità per cui sono legalmente conservati.

Se il Titolare del trattamento non ha espresso contrattualmente la propria scelta, Sodexo chiederà al Titolare di comunicare la propria decisione in merito ai Dati personali al più tardi alla data di risoluzione del contratto.

Infine Sodexo, in qualità di Responsabile del trattamento, informerà ogni entità Sodexo a cui sono stati sub-trattati i Dati personali di qualsiasi cancellazione o anonimizzazione dei dati e richiederà a ciascuna delle suddette entità Sodexo di fare lo stesso.

## Appendice 3 – Procedura di cooperazione delle BCR

1. La presente Procedura di cooperazione stabilisce il modo in cui le entità Sodexo aderenti alle BCR collaboreranno con le rispettive Autorità di controllo competenti per qualsiasi richiesta o questione relativa all'attuazione, interpretazione o applicazione delle BCR.
2. Le entità Sodexo aderenti alle BCR metteranno a disposizione il personale necessario per dialogare con le Autorità di controllo competenti.
3. Le entità Sodexo aderenti alle BCR si conformeranno alle decisioni o ai pareri delle Autorità di controllo competenti in merito a qualsiasi questione relativa alla legge sulla protezione dei dati che possa influire su attuazione, interpretazione o applicazione delle BCR.
4. Le entità Sodexo aderenti alle BCR esamineranno e prenderanno in considerazione attivamente le linee guida, le raccomandazioni e le migliori prassi emesse o approvate dal Comitato europeo per la protezione dei dati che possono influire sull'attuazione, sull'interpretazione o sull'applicazione delle BCR.
5. Le entità Sodexo aderenti alle BCR accettano di attenersi a una decisione formale delle Autorità di controllo competenti in merito a qualsiasi questione relativa all'implementazione, all'interpretazione o all'applicazione delle BCR.
6. Le entità Sodexo aderenti alle BCR comunicheranno senza indebito ritardo alle Autorità di controllo competenti qualsiasi modifica sostanziale alle BCR in conformità alla Procedura di aggiornamento (Appendice 4 delle BCR).
7. Le entità Sodexo aderenti alle BCR risponderanno a qualsiasi richiesta di informazioni o reclamo da parte delle Autorità di controllo competenti.
8. Su richiesta, le entità Sodexo aderenti alle BCR forniranno alle Autorità di controllo competenti una copia dei risultati di qualsiasi valutazione di conformità alle BCR e/o altra documentazione richiesta, e la possibilità di condurre un audit delle entità Sodexo aderenti alle BCR allo scopo di esaminare la conformità alle BCR.

## Appendice 4 – Procedura di aggiornamento delle BCR

### Introduzione

1. La presente Procedura di aggiornamento stabilisce le modalità con cui Sodexo comunicherà le modifiche apportate alle BCR alle Autorità di controllo competenti, ai Clienti, agli interessati e alle entità Sodexo aderenti alle BCR.

### Modifiche sostanziali

2. Sodexo comunicherà tempestivamente qualsiasi modifica sostanziale alle BCR (intesa come qualsiasi modifica che possa influire sul livello di protezione offerto dalle BCR o che influisca significativamente sulle BCR stesse, quali modifiche al carattere vincolante delle BCR) alle Autorità di controllo pertinenti, tramite la *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), che agisce come Autorità di controllo principale di Sodexo.
3. Qualora una modifica sostanziale delle BCR influisca sulle condizioni in cui Sodexo tratta i Dati personali per conto di un Cliente in base ai termini di un contratto o di un altro documento vincolante che Sodexo ha sottoscritto con tale Cliente, Sodexo dovrà:
  - a. comunicare la modifica proposta prima di attuarla, e con un preavviso sufficiente a consentire al Cliente interessato di opporsi; e
  - b. consentire al Cliente di sospendere il trasferimento dei Dati personali a Sodexo e/o di interrompere il suo rapporto con quest'ultima, in conformità con i termini del suo contratto o altro documento vincolante sottoscritto con Sodexo.

### Modifiche amministrative

4. Sodexo comunicherà le modifiche alle BCR di natura amministrativa (comprese le modifiche all'elenco delle entità Sodexo aderenti alle BCR) alle Autorità di controllo competenti, tramite la CNIL, almeno una volta all'anno. Sodexo fornirà anche una breve spiegazione delle ragioni di qualsiasi modifica amministrativa comunicata apportata alle BCR.

### Comunicazione agli Interessati e alle entità Sodexo aderenti alle BCR

5. Sodexo comunicherà senza indebito ritardo tutte le modifiche apportate alle BCR, siano esse di natura amministrativa o sostanziale, alle entità Sodexo aderenti alle BCR e ai Clienti.
6. Sodexo comunicherà le modifiche amministrative o sostanziali agli Interessati che beneficiano delle BCR tramite l'Intranet e il sito web ufficiale di Sodexo.

### **Ruolo del Group Data Protection Officer**

7. Il Group Data Protection Officer, con il supporto del Global Data Protection Office, (i) terrà un elenco completamente aggiornato delle entità Sodexo aderenti alle BCR e dei sub-responsabili coinvolti nelle attività di trattamento dei dati per i Clienti (in qualità di Titolari del trattamento); (ii) renderà accessibile ai Clienti (in qualità di Titolari del trattamento), agli Interessati e alle Autorità di controllo il suddetto elenco completamente aggiornato; e (iii) terrà traccia e registrerà qualsiasi aggiornamento delle BCR e fornirà sistematicamente le informazioni necessarie ai Clienti (in qualità di Titolari del trattamento) e/o alle Autorità di controllo su richiesta.
8. Sodexo garantirà che non venga effettuato alcun trasferimento a una nuova entità di Sodexo fintanto che questa non sia effettivamente vincolata dalle BCR o da altre misure di salvaguardia appropriate e non possa garantire la conformità alle BCR.



## **Appendice 5 – Politica globale sulla protezione dei dati di Sodexo**

Link alla Politica globale sulla protezione dei dati di Sodexo pubblicata sul sito web aziendale di Sodexo SA.

## **Appendice 6 – Politica globale di gestione dei diritti per la protezione dei dati**

Link alla Politica globale di gestione dei diritti per la protezione dei dati pubblicata sul sito web aziendale di Sodexo SA.

## Appendice 7 – Descrizione dell'ambito di applicazione materiale della Processor Policy

Tipologie di Trattamento dei dati personali effettuati e/o previsti e finalità	Categorie di Interessati coinvolti	Categorie di Dati personali trattati	Elenco dei Paesi di destinazione
<ul style="list-style-type: none"> <li>- Prestazione dei servizi forniti da Sodexo per conto dei Clienti (ad esempio, servizi di Facility Management, servizi di ristorazione, alcuni servizi di Benefits &amp; Rewards<sup>11</sup>)</li> </ul>	<ul style="list-style-type: none"> <li>- Clienti (contatti commerciali attuali o potenziali)</li> <li>- Consumatori/Beneficiari (consumatori o beneficiari attuali o potenziali)</li> </ul>	<ul style="list-style-type: none"> <li>- Dati identificativi (stato civile, identità, ecc.)</li> <li>- Vita professionale</li> <li>- Dati di connessione (ad esempio, credenziali per l'autenticazione, log/interazione con le applicazioni IT pertinenti, indirizzo IP)</li> </ul>	<ul style="list-style-type: none"> <li>- Tutti i Paesi in cui operano le entità Sodexo</li> </ul>

<sup>11</sup> Servizi forniti da Sodexo per conto dei Clienti:

- servizi in loco:
  - servizi di ristorazione: catering, caffetteria, ristorazione particolare, attività di ristorazione al dettaglio e distributori automatici;
  - servizi di gestione delle strutture (Facility Management):
    - servizi di Soft Facility Management: pulizia, lavanderia, reception, help desk, sicurezza;
    - servizi di Hard Facility Management: manutenzione tecnica, manutenzione elettrica, manutenzione degli edifici;
- servizi di Benefits & Rewards:
  - vantaggi per i dipendenti: Sodexo elabora buoni pasto (Meal Pass) o buoni regalo (Gift Pass) per attrarre e fidelizzare i dipendenti e migliorare l'efficienza organizzativa;
  - diversificazione: Sodexo offre soluzioni semplici e di facile accesso per affrontare le sfide legate a mobilità, salute e benessere, oltre a incentivi e riconoscimenti attraverso piattaforme uniche come le carte carburante, la prenotazione dei viaggi con Mobility Pass e la gestione delle spese aziendali.

Le entità Sodexo possono essere considerate responsabili del trattamento per questi servizi a seconda della normativa locale.

