MANUAL INTERNO DE DATOS PERSONALES

1. OBJETO

El presente manual tiene el propósito de definir los lineamientos para la implementación, monitoreo, sostenimiento y mejora continua del Programa integral de gestión de datos Personales de SODEXO S.A.S, en adelante el Programa; así como las acciones a seguir para la prevención de incidentes de seguridad y la atención de los mismos. Lo anterior, según lo dispuesto en la Ley 1581 de 2012, las normas que lo modifiquen y complemente y en la Política de Protección de Datos Personales de Sodexo.

Este manual es obligatorio y aplica para todos los procesos de la Compañía involucrados con la protección de datos personales especialmente las áreas de Recursos Humanos, Operaciones, Comercial, Marketing, Legal, Tecnología y cualquier otra que maneje información de terceros, tales como: proveedores, clientes, empleados, accionistas, Representantes Legales, etc.

2. RESPONSABLES

El responsable de cada área de la compañía que tiene como necesidad la utilización de datos personales es responsable de garantizar la implementación de la Política de Protección de Datos Personales, el presente manual, y demás requerimientos de la Ley.

3. SOBRE LA AUTORIZACIÓN PARA EL USO DE DATOS PERSONALES

3.1 DISPOSICIONES GENERALES PARA LA OBTENCIÓN DE LA AUTORIZACIÓN

Toda captura, recolección, uso y almacenamiento de datos personales que realice Sodexo en el desarrollo de sus actividades, y de aquellas finalidades dispuestas en la Política de Protección de Datos Personales, requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado.

Sodexo ha puesto a disposición de los titulares la autorización para el tratamiento de sus datos personales en los diversos escenarios en los cuales realiza la captura del dato, tanto de manera física como digital, a través de formatos de autorización en donde se informa al titular sobre la captura de sus datos personales, el tratamiento al cual serán sometidos incluyendo las finalidades, sus derechos, los canales de ejercicio de sus derechos y la información relacionada sobre la Política de Protección de Datos Personales.

En todos los casos la obtención de la autorización se realizará bajo las diferentes modalidades que establece la ley, teniendo en cuenta la naturaleza de cada uno de los canales de captura de la información, y el modo en que la misma es obtenida, es decir, si es a través de un canal escrito, verbal o mediante una conducta inequívoca.

Es importante tener en consideración que en todos los casos cada área responsable de Sodexo debe custodiar las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la Superintendencia de Industria y Comercio. Así las cosas, se deberán guardar los formatos físicos y/o digitales en donde existan autorizaciones, el registro de llamadas y/o videos, y de los formularios web en los cuales se da trazabilidad sobre la aceptación del tratamiento.

3.2 Modalidades de Autorización. Las modalidades de autorización de tratamiento de datos personales pueden ser tramitados a través de formatos web, apps o documentos físicos.

a. Autorización en Formatos Web y apps

Las áreas que, en el ejercicio de sus funciones, o debido a que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios web, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.

b) La recolección y el envío del formulario web, deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato.

c) Validar que en el la autorización se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.

d) Validar que la plataforma que soporta el formulario web o de la app tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas. Deberá incluir fecha en la que se obtuvo la autorización y la identificación de los titulares.

b. Autorización en medios físicos o digitales

Las áreas que lleven recolecten datos personales a través de medios físicos o digitales, deberán tener en cuenta los siguientes aspectos:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la recolección.

b) Solicitar la autorización del titular de los datos.

c) Validar que en la autorización se encuentren todas las finalidades de tratamiento asociadas a la recolección de los datos solicitados.

d) Garantizar la custodia de los formatos físicos o digitales con sus respectivas autorizaciones.

c. Autorización en la toma de imagen (video y fotografías)

i. Autorización uso de CCTV

Sodexo cuenta con cámaras de video vigilancia que tienen como finalidad dar cumplimiento a las políticas de seguridad física, cumpliendo con los parámetros establecidos en la Guía para la Protección de Datos Personales en Sistemas de Videovigilancia, expedidos por la SIC como autoridad de control.

Con el propósito de cumplir con las disposiciones legales para el tratamiento de datos personales y/o sensibles como la imagen, Sodexo ha dispuesto de avisos de privacidad en sus

instalaciones donde se cuenta con sistema de CCTV de propiedad y/o administrado por **SODEXO**.

La información así obtenida sólo se utilizará con fines de seguridad de los empleados, personas naturales, bienes y activos que en ella se contengan. Dicha información podrá ser utilizada como prueba en cualquier momento que sea requerida, ante cualquier autoridad, institución oficial u organización privada que lo solicite. Esta información será conservada por el plazo establecido en la normativa nacional.

ii. Autorización para eventos y actividades particulares

El área encargada del evento o actividad particular en la cual se capturen imágenes, video, datos biométricos, y/o voz o audio de empleados o terceros, deberá velar por el adecuado cumplimiento de las directrices establecidas sobre protección de datos personales.

El área a cargo del tratamiento de los datos gestionará la autorización del titular para el uso de su imagen, garantizando su custodia. Por último, en cada caso se deberá realizar el análisis sobre la imagen que custodiará Sodexo, dado que, si la misma tiene implicaciones sobre derechos de autor, se deberá contar adicionalmente con el consentimiento del autor para hacer uso de ella.

3.3 Custodia de la autorización

Cada área de Sodexo que realice un tratamiento activo de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos. Así mismo, se deberán poner a disposición de la Superintendencia de Industria y Comercio o del Oficial de Protección de Datos en el evento en que éstos lo requieran.

4. GOBIERNO EN LA PROTECCIÓN DE DATOS PERSONALES

Sodexo dentro de su programa de protección de datos personales ha estructurado unos roles para el desarrollo, verificación y control del programa el cual está constituido por:

a) Oficial de Protección de Datos Personales: Es la persona encargada de liderar el programa a través de: i) la planeación, ejecución y seguimiento de los elementos que hacen parte del programa; ii) asesorar y sensibilizar a los empleados de Sodexo en relación con el programa y las principales obligaciones en su ejecución y desarrollo; iii) emitir conceptos y dar respuesta a las inquietudes y requerimientos sobre protección de datos personales a nivel interno y externo, así como asesorar sobre los asuntos relacionados con el manejo de información personal; iv) realizar el seguimiento de las normas sobre protección de datos personales y realizar las adecuaciones pertinentes al programa para procurar su cumplimiento; v) hacer seguimiento a la correcta implementación del programa en Sodexo, y vi) gestionar y liderar el proceso de actualización de bases de datos ante el Registro Nacional de Bases de Datos y realizar los reportes legales que los entes de control soliciten.

b) Delegados de Protección de Datos Personales: Son las personas encargadas de las bases de datos identificadas y reportadas antes el Registro Nacional de Bases de Datos, quienes tienen el deber de reportar actualizaciones o cambios sustanciales en la información de la base de datos que deba ser reportada ante la Superintendencia de Industria y Comercio. Adicionalmente, están

encargadas de informar sobre cambios en el tratamiento de datos personales, o puntos de captura adicionales que requieran coberturas y de custodiar las Bases de datos.

c) Comité de Protección de Tratamiento de Datos: Está encargado de realizar el seguimiento a los principales temas del programa de protección de datos personales en Sodexo. Es el escenario de control donde se revisan, discuten, validan y aprueban directrices enfocadas a implementar, consolidar y mejorar continuamente las actividades que hacen parte del programa de protección de datos personales. Está integrado por, el Oficial de Protección de Datos Personales de Sodexo, por el Gerente de Administración de RRHH, , Director de Tecnología y Transformación digital, Gerente de IT, Gerente de Cumplimiento y Riesgo, Gerente Proyectos Supply, Gerente de Operaciones, Gerente Comercial, Director y Gerente Legal, Gerente de Inteligencia de Mercados, Jefe de Fidelización, Jefe de Salud Ocupacional, Jefe de Excelencia Operacional

5. PROCEDIMIENTO DE ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS RELACIONADAS CON LA PROTECCIÓN DE DATOS PERSONALES

El procedimiento de consultas y reclamos se ejecutará de acuerdo con los términos incluidos en la ley y acogidos por la Política de Protección de Datos Personales. Las solicitudes que pueden ser catalogadas como consultas o reclamos pueden llegar por los canales habilitados de protección de datos, los cuales son: las oficinas físicas de atención al usuario ubicadas en la Av. Cra 19 No 95-20 Oficina 2601, Teléfono: (+57 1) 7421460, o a través del Correo electrónico: protecciondatospersonales.fms.co@sodexo.com

Los tiempos de respuesta de las consultas serán de diez (10) días hábiles desde la fecha de recibo, y de los reclamos serán de quince (15) días hábiles desde su recibo.

6. ACREDITACIÓN DEL PRINCIPIO DE LA RESPONSABILIDAD DEMOSTRADA (“ACCOUNTABILITY”) Y EL RELACIONAMIENTO CON TERCEROS

Para llevar a cabo un adecuado tratamiento de los datos personales, las diferentes áreas que hagan tratamiento de datos deberán validar los siguientes elementos de manera periódica:

a) Revisión de las actividades que generan algún tipo de tratamiento de los datos personales

b) Validación de los puntos de recolección de información personal, identificando el tipo de información que se recolecta y sus finalidades

c) Inventario y actualización de las bases de datos identificadas

d) Seguimiento al cumplimiento de las medidas de seguridad de las bases de datos y repositorios de información que se encuentren en el inventario

e) Identificación de terceros que realizarán el tratamiento de datos personales.

En los contratos que Sodexo suscriba se incorporarán cláusulas de protección de datos personales, y adicionalmente, se podrá solicitar a los terceros en el desarrollo del vínculo comercial o contractual, información que permita validar el cumplimiento de las directrices contenidas en la Política de Protección de Datos Personales de Sodexo, así como aquellas directrices legales y reglamentarias, cuando se estime necesario.

Los terceros que realicen un tratamiento de datos personales de los cuales Sodexo es responsable, deberán acreditar el cumplimiento de los requisitos del régimen de protección de datos personales, aportando: i) la política de protección de datos personales; ii) información sobre los canales habilitados para el trámite de consultas y reclamos y iii) el cumplimiento sobre el registro de las bases de datos ante el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio.

Sin perjuicio de lo anterior, Sodexo podrá realizar verificaciones aleatorias en el desarrollo del vínculo comercial o contractual para validar que se esté efectivamente cumpliendo con las disposiciones de protección de datos, por lo cual se podrá solicitar evidencias o soportes del cumplimiento.

7. PROGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN

Conforme a lo definido por Sodexo, se realizará una capacitación anual relacionada con la protección de los datos personales.

8. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES CON DATOS PERSONALES

Se entiende por incidente la violación de las medidas de seguridad que recaiga sobre las bases de datos personales.

Sodexo adoptará todas las medidas de seguridad correspondientes para proteger los datos personales entregados para su custodia bien sea como Responsable y/o Encargado, así como cualquier otra conducta que constituya un tratamiento inadecuado de datos personales en contravía de lo aquí dispuesto o de lo señalado en la Ley.

En caso de conocer alguna incidencia ocurrida deberá comunicarse **inmediatamente** al Oficial de Protección de Datos quien adoptará las medidas oportunas frente al incidente reportado.

Las incidencias pueden afectar tanto a bases de datos digitales como físicas y generarán las siguientes actividades:

a. Notificación de Incidentes

Cuando se presuma que un incidente pueda afectar o haber afectado a bases de datos con información personal se deberá informar al Oficial de Protección de Datos Personales quién analizará y de ser necesario gestionará su reporte en el Registro Nacional de Bases de Datos.

b. Gestión de Incidentes

Es responsabilidad de cada empleado, contratista, consultor o tercero, reportar de manera oportuna cualquier violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de **Sodexo.**

c. Identificación

Todos los incidentes de seguridad, tales como aquellos en los que se observe el potencial de perdida de reserva o confidencialidad de la información, deben ser evaluados para determinar si son o no, un incidente y deben ser reportados al Comité de Datos Personales.

El Comité De Protección De Datos Personales deberá activar a el área de IT, conjuntamente con el Oficial de Protección de Datos Personales y las área usuaria de la información, quienes deberán levantar el informe y establecer el procedimiento a seguir ante la situación presentada

d. Reportes y comunicaciones

Reporte a la Autoridad de Datos Personales:

El Oficial de Protección de Datos Personales evaluará y en el evento de confirmarse una violación o afectación a los datos personales, informará a LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, dentro de los 15 días (o el término que establezca la autoridad) a partir del conocimiento de esta.

Los empleados deben reportar a su jefe directo y al Oficial de Protección de Datos Personales cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de **Sodexo.**

Reporte al Grupo SODEXO:

Adicionalmente, El Oficial de Protección de Datos Personales debe registrar el reporte en la plataforma One trust o la que el grupo SODEXO designe; las circunstancias de modo, tiempo y lugar del incidente, Fecha de conocimiento del incidente, Calidad de Sodexo de responsable o Encargado de las Bases de Datos, si se informó a los titulares y clientes, categoría de titulares e información vulnerada entre otros y en general toda la información que requiera la herramienta para generar el reporte del incidente.

Comunicar a los Titulares de la información

En caso que se presente un Incidente de seguridad que genere una violación o afectación a los datos personales, Sodexo deberá informar al Titular de la Información del Incidente con el fin de que conozca de la ocurrencia del mismo y las posibles consecuencias y las acciones tomadas por la compañía para mitigar el riesgo; y, brindarles la oportunidad para que ellos mismos puedan adoptar las medidas necesarias para protegerse de las consecuencias de un incidente de seguridad.

e. Contención, Investigación y Diagnostico

El Oficial de Protección de Datos Personales debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado. En caso de que se identifique un delito informático, en los términos establecidos en la Ley 1273 de 2009, el Oficial de Protección de Datos Personales, reportará tal información a las autoridades de investigaciones judiciales respectivas.

f. **Plan de acción**

El área comprometida, los directamente responsables de la gestión de datos personales y el área de IT , deben prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades existentes y generando un plan de acción.

g. Cierre de Incidente y Seguimiento

El área de IT, conjuntamente con el Oficial de Protección de Datos Personales y las área usuaria de la información, iniciarán y documentarán todas las tareas de revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad.

El Oficial de Protección de Datos Personales preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

9. VERIFICACIÓN DEL CUMPLIMIENTO DE LAS DISPOSICIONES SOBRE DATOS PERSONALES

El Oficial de Protección de Datos Personales podrá, en cualquier momento, adelantar auditorías de supervisión de cumplimiento de las disposiciones sobre protección de datos personales, con el propósito de garantizar el adecuado cumplimiento y desarrollo del programa. Como resultado de las revisiones pueden levantarse planes de acción para cerrar las brechas encontradas, los cuales tendrán seguimiento en los Comités de Protección de Datos.

8. PERMANENCIA Y ACTUALIZACIÓN DE LA DATA

La permanencia de las bases de datos será tratada de acuerdo con lo dispuesto en el **Anexo No 1 de Permanencia de los datos.**

La base de datos se actualizarán i) Cada vez que se realicen cambios sustanciales en la información consignada en el Registro Nacional de Bases de Datos (RNBD) ii) Cada vez que se genere una nueva base de datos y iii) Anualmente en el término dispuesto por la Superintendencia de Industria y Comercio para realizar la actualización.

VIGENCIA

El procedimiento descrito en el presente documento se aplicará a partir de su publicación.

ANEXO NO 1 DE PERMANENCIA DEL DATO

Las bases de datos que se encuentran registradas en el Registro Nacional de Base de Datos son las siguientes:

Nombre de la Base de datos
Empleados – Documentos
Proveedores Compras – Documentos
Proveedores Compras
Clientes – Documentos
Empleados Nómina
Clientes
Junta Directiva/Accionistas

La permanencia de los datos en las respectivas bases de datos será la siguiente:

- Para la base de datos de empleados la permanencia de los datos será de 20 años.
- Para datos contables la permanencia será de 20 años.
- Para datos relacionados con la pensión será de 80 años.
- Para las demás bases de datos la permanencia de los datos será de 10 años.

Estos plazos se empezarán a contar desde la desvinculación del colaborador para la base de datos de empleados, y desde la fecha de terminación o liquidación del contrato para las demás bases de datos