Resolución Directoral N°3557-2019-JUS/DGTAIPD-DPDP

Expediente N°
006-2019-JUS/DGTAIPD-PAS

Lima, 29 de noviembre de 2019

VISTOS:

El Informe Final de Instrucción Nº 058-2019-JUS/DGTAIPD-DFI[1] del 31 de mayo de 2019, emitido por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la "DFI"), y demás documentos que obran en el respectivo expediente, y;

CONSIDERANDO:

I. Antecedentes

1. Mediante la Orden de Visita de Fiscalización Nº 064-2018-JUS/DGTAIPD-DFI[2] de fecha 11 de junio de 2018, la DFI dispuso la realización de una visita de fiscalización a SERVICIOS DE CALL CENTER DEL PERÚ S.A., identificada con R.U.C. N° 20519395224, dedicada a brindar servicios de gestión de llamadas y call center (en adelante, la administrada), a fin de verificar el cumplimiento de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP") y su reglamento, aprobado por Decreto Supremo N° 003-2013-JUS (en adelante, el "Reglamento de la LPDP")

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

2. Dicha visita se efectuó el 18 de junio de 2018, en la sede ubicada en Jr. Camaná N°678, Lima, durante la cual, se verificó lo siguiente:

2.1. Que, la administrada cuenta con cinco (5) bancos de datos personales denominados i) "Colaboradores", ii) "Personas", iii) "Reclutamiento", iv) "Control de Acceso Físico" y v) "Videovigilancia". Dichos bancos de datos están inscritos en el Registros Nacional de Protección de Datos Personales.

2.2. Respecto al banco de datos "Personas" fiscalizado:

2.2.1. La administrada informó que tiene un contrato con la empresa Oncosalud para la captación de nuevos clientes. Asimismo, indicó que en el marco de dicho contrato, a través de un contrato con la empresa Infocore S.A.C (en adelante, "Infocore") adquiere banco de datos personales.

2.2.2. Se verificó que Infocore remite los datos personales: números de DNI y números telefónicos mediante el aplicativo (sistema) MOVEIT.

[1] Folio 506 al 515
[2] Folio 18

2.2.3. Se verificó que el tratamiento del banco de datos "Personas" se realiza en soporte automatizado, en dos sedes o locaciones. El tratamiento automatizado es realizado por los sistemas MOVEIT, CRM, SICCAB (CRM) y el aplicativo Microsoft Excel.
2.2.4. Se verificó que el servicio de mesa de ayuda es realizado por la administrada.
2.2.5. Se verificó que no cuenta con aplicativos móviles que realicen tratamiento del banco de datos "Personas".
2.2.6. Respecto al sistema MOVE IT, se verificó que es de tipo web y propiedad de la empresa IPSWITCH, sin embargo, el servidor físico se encuentra en la entidad fiscalizada. Se generan registros de interacción lógica de las acciones relevantes, mas no de los inicios y cierres de sesión de los usuarios. No se realizan copias de respaldo de dicho sistema. El sistema MOVE IT cuenta con un registro superior a mil (1 000) datos personales.
2.2.8. Respecto al sistema CRM, se verificó que realizan copias de respaldo semanalmente en cintas TAPE LTO a cargo del coordinador de servidores, quien es responsable de verificar la integridad de las copias de respaldo. Se verificó que tienen un contrato de custodia con la empresa Iron Mountain para el almacenamiento de las cintas TAPE LTO. El sistema CRM genera y mantiene registro de interacción lógica (inicio, cierre de sesión y acciones relevantes). El sistema CRM cuenta con un registro de noventa y seis mil doscientos treinta y dos (96 232) datos personales.
2.2.9. Respecto al aplicativo Microsoft Excel, se verificó que genera registros de interacción lógica y que se realizan copias de respaldo al servidor de archivos donde se encuentra alojado dicho aplicativo.
2.2.10. Respecto al sistema SICCAB-CRM, se verificó que su función es cargar los datos personales del aplicativo Microsoft Excel al sistema CRM, además consignan los accesos del aplicativo.
2.2.11. Se constató que para el acceso al centro de datos donde se alojan los sistemas MOVEIT, CRM y el aplicativo Microsoft Excel se requiere la validación a través de un lector biométrico a cargo del coordinador de redes. Dicho centro de datos se encuentra en un ambiente aislado, contando con: Sistema de detección y protección de incendio FM200, tablero eléctrico, falso piso, aire acondicionado de precisión, VPS, grupo electrógeno, cámara de videovigilancia, extintores vigentes, gabinetes con llave (para servidores) a cargo del coordinador de servidores.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

3. En la segunda visita de fiscalización, en la sede ubicada en Jr. Camaná, que consta en el Acta N° 02-2018 de fecha 2 de julio de 2018, se verificó lo siguiente:

3.1. Respecto al tratamiento del banco de datos "Personas":
3.1.1. Se verificó que el sistema CRM asigna aleatoriamente al ejecutivo de ventas de la administrada para que realice la llamada telefónica y ofrezca los servicios de Oncosalud. En dicha llamada el ejecutivo de ventas solicita los datos personales (nombres, DNI, edad, fecha de nacimiento, dirección, condición de fumador, antecedentes de cáncer personal y familiares)
3.1.2. Los datos son enviados al área de validación quien certifica la venta, y luego de la validación, se envía la información a Oncosalud.
3.2. Que, los ejecutivos de ventas cuentan con locker para el almacenamiento de sus celulares, dado que cuentan con políticas de escritorio limpio.
3.3. Que, la sede fiscalizada no cuenta con impresoras o equipo de reproducción de documentos.
3.4. Que, el coordinador de ventas tiene asignado el sistema CCPULSE a través del cual monitorea a los ejecutivos de ventas.

3.5. Que, el sistema CCPULSE no almacena datos personales de clientes de Oncosalud.

4. En la tercera visita de fiscalización, en la sede ubicada en Av. España N°382, Cercado de Lima, que consta en el Acta N° 03-2018 de fecha 2 de julio de 2018, se verificó lo siguiente:

4.1. Que, el sistema MOVE IT no realiza copias de respaldo. Dicho sistema sólo es usado con la finalidad de realizar transferencias de datos personales a través del protocolo de transferencia seguro SFTP. Los datos personales son alojados en el sistema CRM del cual sí se realizan copias de respaldo.
4.2. Que, la administrada transfiere los datos personales a Oncosalud, a través de tramas encriptadas y con contraseña.
4.3. Que, el sitio web www.scc.com.pe es de titularidad de la administrada y que recopila datos personales a través de los formularios "Ponte en Contacto", "Buzón de Propuesta" e "Ingresa tu CV".
4.4. Que, el formulario "Ponte en Contacto" sólo recopila datos de personas jurídicas. En cuanto a los formularios "Buzón de Propuesta" e "Ingresa tu CV", la información es recopilada por la Coordinadora de Comunicación y Desarrollo Humano, quien recibe los datos personales a través del panel de administración del sitio web; dichos datos son almacenados en el Banco de datos "Colaboradores"
4.5. La administrada informó que el servidor físico de los formularios señalados en el numeral 4.4 se encuentra en Estados Unidos de América.
4.6. Que, la administrada se encuentra en proceso de inscripción de la comunicación de flujo transfronterizo de datos personales.
4.7. Que, la administrada no realiza transferencia nacional ni internacional del banco de datos "Personas".
4.8. Que, el sistema MOVE IT genera registros de interacción lógica (inicio y cierre de sesión)
4.9. Que, el tiempo de tratamiento del banco de datos "Personas" es indeterminado.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

5. En el Informe Técnico N° 000187-2018-DFI-VARS del 23 de agosto de 2018[3], el Analista de Fiscalización en Seguridad de la Información concluyó lo siguiente sobre la administrada:

5.1. Que, la administrada realiza flujo transfronterizo de los datos personales recopilados a través de los formularios "Buzón de Propuesta" e "Ingresa tu CV de su sitio web www.scc.com.pe, dado que el servidor físico que aloja la información se encuentra en Estados Unidos de América.
5.2. Que, la administrada no publica en su sitio web www.scc.com.pe "Términos y Condiciones" y "Políticas de Privacidad".
5.3. Que, documenta adecuadamente los procedimientos de gestión de accesos, gestión de privilegios y la verificación periódica de privilegios asignados, cumpliendo con el numeral 1 del artículo 39 del Reglamento de la LPDP.
5.3. Que, genera y mantiene registros de evidencias producto de la interacción lógica, cumpliendo con el numeral 2 del artículo 39 del Reglamento de la LPDP.
5.4. Que, dispone de un ambiente donde se almacena, procesa, transmite información de datos personales. Tal centro de datos cuenta con las medidas de seguridad adecuadas, cumpliendo con el primer párrafo del artículo 40 del Reglamento de la LPDP.

[3] Folios 209 al 212

5.5. Que, garantiza el respaldo de la información del banco de datos personales "Personas" a través de generación de copias seguras y continuas, cumpliendo con el segundo párrafo del artículo 40 del Reglamento de la LPDP.

6. Mediante Proveído de 15 de octubre de 2018 la DFI dispuso ampliar el plazo de fiscalización por cuarenta y cinco (45) días hábiles adicionales, a partir del 26 de octubre de 2018.

7. En la cuarta visita de fiscalización, en la sede ubicada en Jr. Camaná, que consta en el Acta N° 04-2018 de fecha 30 de octubre de 2018, se reportó lo siguiente:

7.1. La administrada informó que mantiene contrato vigente con las empresas: Banco Scotiabank, Entel, BBVA y Oncosalud.

7.2. Respecto al servicio que brinda a GSP Servicios Comerciales S.A.C (en adelante "GSP"), la administrada informó que la gestión de venta de seguros oncológicos de Oncosalud se realiza con un banco de datos de prospectos de clientes generado por la administrada y con los bancos de datos personales provistos por Interbank y Saga Falabella.

7.3. Respecto al banco de datos generado por la administrada utilizado para la venta de seguros oncológicos de Oncosalud, se verificó que es obtenido a través del sistema web de importación de datos Infocore, en el cual se deben ingresar los números de DNI para la obtención de los números telefónicos asociados a los mismos. Los números de DNI son descargados del enlace http://dniperu.online/ y el procedimiento está descrito en el documento denominado "Proceso de obtención de información a través del Sistema de Importación de datos Infocore".

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

8. En la quinta visita de fiscalización, en la sede ubicada en Jr. Camaná, que consta en el Acta N° 05-2018 de fecha 8 de noviembre de 2018, se reportó lo siguiente:

8.1. La administrada precisó que mantiene contrato con las siguientes empresas: i) Banco Scotiabank, a quien brinda el servicio de venta de tarjetas de crédito y compra de deuda, ii) Entel Perú S.A, a quien brinda el servicio de televentas (portabilidad), iii) BBVA Banco Continental, a quien brinda el servicio de venta de tarjetas de crédito y préstamos personales, iv) Oncosalud, a quien brinda el servicio de venta de seguros oncológicos. La administrada mencionó que también realiza la venta de seguros de Oncosalud, utilizando un banco de datos personales provisto por Scotiabank. Asimismo, se verificó que el tratamiento y envío de la información es realizado de acuerdo a lo indicado en el documento "Matriz de tratamiento y envío de información (A)"

8.2. Se recopiló muestras de las llamadas telefónicas realizadas por los teleoperadores para el ofrecimiento de productos de Scotiabank, Entel Perú S.A y BBVA Banco Continental.

8.3. La administrada informó que el tratamiento de información (correspondiente a las ventas de seguros oncológicos de Oncosalud) es realizado en su sede de la Av. España N°382, Cercado de Lima.

9. En la sexta visita de fiscalización, efectuada en la sede de la Av. España, que consta en el Acta N° 06-2018 de fecha 8 de noviembre de 2018, se reportó lo siguiente:

9.1. Se verificó que las ventas de seguros oncológicos de Oncosalud, son realizadas con bancos de datos personales provistos por Interbank, Banco Falabella, Banco Scotiabank y por el banco de datos generado por la

administrada (cuyo medio de obtención se encuentra descrito en el Acta N°04-2018)

9.2. Se verificó que el tratamiento y envío de información es realizado de acuerdo a lo indicado en el documento "Matriz de tratamiento y envío de información (B)".

9.3. Se recopiló muestras de las llamadas telefónicas realizadas por los teleoperadores para el ofrecimiento de productos de Oncosalud. El personal de fiscalización solicitó grabaciones de ventas realizadas los días 29, 30 y 31 de octubre de 2018 (8 audios por día)

9.4. El personal de fiscalización solicitó grabaciones de ventas de productos de Banco Scotiabank, Entel Perú S.A y BBVA Banco realizadas los días 29, 30 y 31 de octubre de 2018 (2 audios por servicio prestado y por día)

10. Por medio del Informe de Fiscalización N° 004-2019-JUS/DGTAIPD-DFI-AARM del 3 de enero de 2019[4], se remitió a la DFI el resultado de la fiscalización realizada, adjuntando los documentos que forman el expediente administrativo, que contó con las siguientes conclusiones:

"**1. SERVICIOS DE CALL CENTER DEL PERÚ S.A.C.** estaría realizando tratamiento de datos personales de los usuarios de su sitio web sin informarles lo requerido por el artículo 18 de la LPDP, lo que vulneraría su derecho de información sobre las condiciones del tratamiento de sus datos personales. Hecho que constituiría una presunta infracción, según lo regulado en el literal a, numeral 2, artículo 132 del RLPDP: *"No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley N° 29733 y su Reglamento"*, dicha infracción es **grave** conforme al citado artículo.

2. SERVICIOS DE CALL CENTER DEL PERÚ S.A.C. no contaría con consentimiento válido de los titulares de los datos personales almacenados en el banco de datos personales denominado "prospecto de clientes" para recopilarlos y usarlos para telemarketing. Hecho que constituiría una presunta infracción, según lo regulado en el literal b, numeral 2, artículo 132 del RLPDP, esto es, *"Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea conforme a lo dispuesto en la Ley N° 29733 y su Reglamento"*, dicha infracción es **grave** conforme al citado artículo.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

3. SERVICIOS DE CALL CENTER DEL PERÚ S.A.C. no habría inscrito el banco de datos personales de usuarios de su sitio web ante el Registro Nacional de Protección de Datos Personales. Hecho que constituiría una presunta infracción, de conformidad con el literal e. numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el registro Nacional los actos establecidos en el artículo 34 de la Ley"*, dicha infracción es **leve** conforme al citado artículo.

4. SERVICIOS DE CALL CENTER DEL PERÚ S.A.C., no habría comunicado la realización de flujo transfronterizo ante el Registro Nacional de Protección de Datos Personales. Hecho que constituiría una presunta infracción, de conformidad con el literal e. numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el registro Nacional los actos establecidos en el artículo 34 de la Ley"*, dicha infracción es **leve** conforme al citado artículo."

11. Dicho Informe de Fiscalización fue notificado el 28 de enero de 2019 a la administrada mediante Oficio N° 62-2019-JUS/DGTAIPD-DFI[5].

[4] Folios 309 al 320
[5] Folios 322 y 323

12. A través del escrito ingresado con Hoja de Trámite N° 15314-2019[6] del 1 de marzo de 2019; la administrada presentó sus descargos señalando lo siguiente:

12.1. Que, ha incorporado una Política de Privacidad en su plataforma web para los diversos enlaces donde realizan tratamiento de datos personales.
12.2. Que, ha solicitado la inscripción del banco de datos personales titulado "Clientes", en el cual se almacena la información recibida a través del enlace "Ponte en contacto"
12.3. Que, los datos recabados a través del enlace "Buzón de Propuestas", provienen exclusivamente de nuestros colaboradores, por lo que cualquier información remitida a través de dicho link es almacenada en el banco de datos "Colaboradores", no siendo necesaria la inscripción de un banco de datos adicional.
12.4. Que, los datos obtenidos a través del enlace "Ingresa tu CV" son tratados por Bumeran.com Perú S.A.C., quien procesa los perfiles que se adecuan a las ofertas laborales que publica la administrada. Seleccionados los perfiles que podrían adecuarse a los puestos requeridos, dicha información es almacenada en el banco de datos "Reclutamiento", el cual se encuentra inscrito.
12.5. Que, el banco de datos "Colaboradores" se encuentra inscrito para realizar flujo transfronterizo a los países de Chile y Estados Unidos de América, inscrito con código RNPDP-PJP N°2778.
12.6. Que, respecto al banco de datos "Reclutamiento" ha solicitado la modificación del banco incluyendo flujo transfronterizo a Estados Unidos de América.
12.7. Que, respecto al banco de datos "Clientes" ha solicitado la inscripción de realización de flujo transfronterizo de los datos almacenados en éste

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

13. Por medio de la Resolución Directoral N° 040-2019-JUS/DGTAIPD-DFI del 21 de marzo de 2019[7], la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión los siguientes hechos infractores:

i) La administrada estaría recopilando y usando datos personales para la gestión de venta de los planes oncológicos de Oncosalud (telemarketing) sin obtener válidamente el consentimiento del titular de los datos. Obligación establecida en el artículo 13, numeral 13.5 de la LPDP y el artículo 12 del Reglamento de la LPDP.
ii) La administrada no habría cumplido con inscribir en el Registro Nacional de Protección de Datos Personales, el banco de datos personales de usuarios del sitio web www.scc.com.pe, detectado en la fiscalización. Obligación establecida en el artículo 78 del Reglamento de la LPDP.
iii) La administrada no habría comunicado a la DGTAIPD para su inscripción en el Registro Nacional de Protección de Datos Personales el flujo transfronterizo que realiza de los datos personales recopilados en el sitio web www.scc.com.pe, debido a que el servidor físico que aloja la información del sitio web se ubica en Estados Unidos de América. Obligación establecida en el artículo 26 del Reglamento de la LPDP.

14. Mediante el Oficio N° 259-2019-JUS/DGTAIPD-DFI[8], se notificó dicha Resolución Directoral a la administrada el día 1 de abril de 2019.

[6] Folios 327 al 329
[7] Folios 400 al 408
[8] Folios 409 al 410

15. A través del escrito ingresado con Hoja de Trámite N° 28688-2019 del 24 de abril de 2019[9], la administrada presentó sus descargos, señalando lo siguiente:

15.1. Que, el 1 de marzo de 2019, presentó un escrito, por medio del cual informó las acciones tomadas por la administrada en atención a las observaciones y recomendaciones establecidas en el Informe de Fiscalización N°004-2019-JUS/DGTAIPD-DFI-AARM.
15.2. Que, respecto a la primera imputación que nace del vínculo existente entre la administrada e Infocore, la administrada procedió a resolver por mutuo disenso el contrato suscrito con Infocore con anterioridad a la notificación del inicio del procedimiento sancionador.
15.3. Que, suscribió un contrato nuevo con Infocore, mediante el cual ya no remite base de datos con nombres y DNI, sino que Infocore queda obligado a transferir únicamente números telefónicos (celulares y fijos) no relacionados, obtenidos de fuentes de acceso al público, mediante modo seguro.
15.4. Que, respecto a los números telefónicos que Infocore les remita, la administrada realizará el primer contacto y solicitará oportunamente el consentimiento de su titular, conforme al Oficio N°749-2018-JUS/DGTAIPD.
15.5. Respecto a la segunda imputación y tercera imputación, la administrada reiteró los alegatos presentados con Hoja de Trámite N° 15314-2019 del 1 de marzo de 2019.

16. Por medio de la Resolución Directoral N° 089-2019-JUS/DGTAIPD-DFI[10] del 31 de mayo de 2019, la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

17. Mediante Informe N° 058-2019-JUS/DGTAIPD-DFI del 31 de mayo de 2019[11], la DFI remitió a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DPDP) los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

- Imponer una multa ascendente a treinta y dos coma cinco unidades impositivas tributarias (32,5 UIT), por el cargo acotado en el hecho imputado N° 1 a la administrada, por la infracción grave prevista en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley Nº 29733 y su Reglamento"*.
- Imponer una multa ascendente a cero coma cinco unidades impositivas tributarias (0,5 UIT), por el cargo acotado en el hecho imputado N° 2 a la administrada, por la infracción leve prevista en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*
- Imponer una multa ascendente a cero coma cinco unidades impositivas tributarias (0,5 UIT), por el cargo acotado en el hecho imputado N° 3 a la administrada, por la infracción leve prevista en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley"*

[9] Folios 442 al 451
[10] Folios 501 al 503
[11] Folios 506 al 515

18. A través del escrito ingresado con Hoja de Trámite N° 45468-2019 del 27 de junio de 2019[12], la administrada presentó los siguientes descargos:

18.1. Que, actualmente, e incluso antes de la imputación de cargos, no transfiere datos personales a Infocore.

18.2. Que, desde la suscripción del último contrato con Infocore (1 de marzo de 2019), únicamente recibe números telefónicos obtenidos de fuentes de acceso público, sin que para ello remita algún tipo de información que identifique a los titulares de dichos números. Recibidos los números telefónicos, la administrada realiza el primer contacto con la finalidad de obtener de forma válida el consentimiento de los titulares para el tratamiento de sus datos personales.

18.3. Que, respecto a la fecha cierta del nuevo contrato entre la administrada e Infocore, al haber sido observada por la Autoridad indicando que al ser un documento privado no reviste de categoría de fecha cierta conforme lo establecido en el artículo 245 del Código Procesal Civil, la administrada considera que este no es aplicable.

18.4. Que, la Dirección debió remitirse a los principios establecidos en el TUO de la LPAG, si su norma especial tiene deficiencias en la evaluación de medios probatorios. El artículo VIII del TUO de la LPAG precisa que las autoridades administrativas *"no podrán dejar de resolver las cuestiones que se les proponga, por deficiencia de sus fuentes; en tales casos, acudirán a los principios del procedimiento administrativo previstos en esta Ley; en su defecto, a otras fuentes supletorias del derecho administrativo, y sólo subsidiariamente a éstas, a las normas de otros ordenamientos que sean compatibles con su naturaleza y finalidad."*

18.5. Que, se debió considerar el Principio de Presunción de Veracidad en cuanto a que *"En la tramitación del procedimiento administrativo, se presume que los documentos y declaraciones formulados por los administrados en la forma prescrita por esta Ley, responden a la verdad de los hechos que ellos afirman. Esta presunción admite prueba en contrario."*

18.6. Que, respecto a los principios de la potestad sancionadora, en virtud de la presunción de licitud *"Las entidades deben presumir que los administrados han actuado apegados a sus deberes mientras no cuenten con evidencia en contrario."*

18.7. Que, la Dirección debió tomar como cierto los medios probatorios presentados: la resolución por mutuo disenso entre la administrada e Infocore y el nuevo contrato entre ambas del 1 de marzo de 2019, salvo prueba en contrario que no ha sido presentada en el presente procedimiento.

18.8. Que, la suscripción de los contratos entre la administrada e Infocore se realizó dentro del marco de las reglas de la buena fe. La administrada viene recibiendo la información de Infocore, esperando a que ésta actúe de acuerdo a las obligaciones asumidas contractualmente (datos obtenidos de fuentes de acceso público y cuya recopilación se realiza bajo los parámetros legales vigentes).

18.9. Que, del último contrato de 1 de marzo de 2019, tuvo como objeto utilizar la experiencia de Infocore para acceder a diversas fuentes de acceso al público y permitir que, posteriormente, la administrada pueda realizar el primer contacto para la búsqueda del consentimiento del titular en cuanto al tratamiento de sus datos.

18.10. Que, la Autoridad no ha indicado la imposibilidad de utilizar a un tercero para la obtención de los números telefónicos que permitan a los proveedores de

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ I.

[12] Folios 517 al 529

servicios realizar el primer contacto, razón por la cual no debería imputarse una infracción por este hecho.

18.11. Sobre los mecanismos de supresión de datos personales, la administrada sí cuenta con un mecanismo ante la oposición de un usuario al tratamiento de sus datos. Consiste en una lista negra en la que se incluyen los números telefónicos que no pueden ser contactados.

18.12. Que, se ha señalado que no ha existido intencionalidad de enmienda por parte de la administrada, lo cual resulta falso, en tanto se suscribió un nuevo contrato con Infocore el 1 de marzo de 2019, a fin de dar cumplimiento a la regulación vigente en protección de datos personales.

18.13. Que, en un pronunciamiento previo hecho por la Autoridad, Resolución Directoral N°770-2019-JUS/DGTAIPD-DPDP de fecha 25 de marzo de 2019, donde también se analizaba la imposición de una multa por la comisión de una infracción grave, la denunciada fue sancionada con una multa de 5.5UIT, caso en donde también se determinó que no existe un perjuicio económico causado y reincidencia por parte del administrado, como ocurre en el presente caso.

18.14. Que, ha solicitado la inscripción del banco de datos personales titulado "Clientes", en el cual se almacena la información recibida a través del enlace "Ponte en Contacto" (nombres, apellidos, correo electrónico y teléfono)

18.15. Que, los datos recabados a través del enlace "Buzón de Propuestas", provienen exclusivamente de nuestros colaboradores, por lo que cualquier información remitida a través de dicho link es almacenada en el banco de datos "Colaboradores", no siendo necesaria la inscripción de un banco de datos adicional.

18.16. Que, los datos obtenidos a través del enlace "Ingresa tu CV" son tratados por Bumeran.com Perú S.A.C., quien procesa los perfiles que se adecuan a las ofertas laborales que publica la administrada. Seleccionados los perfiles que podrían adecuarse a los puestos requeridos, dicha información es almacenada en el banco de datos "Reclutamiento", el cual se encuentra inscrito.

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ I.

18.17. Que, el banco de datos "Colaboradores" se encuentra inscrito para realizar flujo transfronterizo a los países de Chile y Estados Unidos de América, inscrito con código RNPDP-PJP N°2778.

18.18. Que, respecto al banco de datos "Clientes" ha solicitado la inscripción de realización de flujo transfronterizo de los datos almacenados en éste, conforme se ha informado, incluso antes del inicio del presente procedimiento.

18.19. Que, respecto al banco de datos "Reclutamiento" ha solicitado la modificación del banco incluyendo flujo transfronterizo a Estados Unidos de América, información puesta a disposición de la Autoridad, incluso antes del inicio de este procedimiento.

18.20. Que, si bien el artículo 126 del Reglamento de la LPDP establece que las acciones de enmienda son consideradas atenuantes, esto no se presenta en este caso, ya que la administrada cumplió con subsanar la conducta antes del inicio del procedimiento sancionador.

II. Competencia

19. De conformidad con el artículo 74 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N° 013-2017-JUS, la DPDP es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la DFI.

20. En tal sentido, la autoridad que debe conocer el presente procedimiento sancionador, a fin de emitir resolución en primera instancia, es la Directora de Protección de Datos Personales.

III. Normas concernientes a la responsabilidad de la administrada

21. Acerca de la responsabilidad de la administrada, se deberá tener en cuenta que el literal f) del numeral 1 del artículo 257 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS (en adelante, la "LPAG"), establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del hecho imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos[13].

22. Asimismo, se debe atender a lo dispuesto en el artículo 126 del Reglamento de la LPDP, que considera como atenuantes la colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones conjuntamente con la adopción de medidas de enmienda; dichas atenuantes, de acuerdo con la oportunidad del reconocimiento y las fórmulas de enmienda, pueden permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP[14].

23. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG[15], que establece como condición atenuante el reconocimiento de la responsabilidad por parte del infractor de forma expresa y por escrito, debiendo reducir la multa a imponérsele hasta no menos de la mitad del monto de su importe; y, por otro lado, las que se contemplen como atenuantes en las normas especiales.

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

IV. Cuestiones en discusión

24. Para emitir pronunciamiento en el presente caso, se debe determinar lo siguiente:

24.1. Si la administrada es responsable por los siguientes hechos infractores:

i) La administrada estaría recopilando y usando datos personales para la gestión de venta (telemarketing) sin obtener válidamente el consentimiento del titular de los datos. Obligación establecida en el artículo 13, numeral 13.5 de la LPDP y el artículo 12 del Reglamento de la LPDP.

---

[13] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"**Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**
1.- Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes:
(...)
f) La subsanación voluntaria por parte del posible sancionado del acto u omisión imputado como constitutivo de infracción administrativa, con anterioridad a la notificación de la imputación de cargos a que se refiere el inciso 3) del artículo 255."

[14] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"**Artículo 126.- Atenuantes.**
La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley."

[15] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 004-2019-JUS**
"**Artículo 257.- Eximentes y atenuantes de responsabilidad por infracciones**
(...)
2.- Constituyen condiciones atenuantes de la responsabilidad por infracciones las siguientes:
a) Si iniciado un procedimiento administrativo sancionador el infractor reconoce su responsabilidad de forma expresa y por escrito.
En los casos en que la sanción aplicable sea una multa esta se reduce hasta un monto no menor de la mitad de su importe.
b) Otros que se establezcan por norma especial."

ii) La administrada no habría cumplido con inscribir en el Registro Nacional de Protección de Datos Personales, el banco de datos personales de usuarios del sitio web www.scc.com.pe, detectado en la fiscalización. Obligación establecida en el artículo 78 del Reglamento de la LPDP.

iii) La administrada no habría comunicado a la DGTAIPD para su inscripción en el Registro Nacional de Protección de Datos Personales el flujo transfronterizo que realiza de los datos personales recopilados en el sitio web www.scc.com.pe, debido a que el servidor físico que aloja la información del sitio web se ubica en Estados Unidos de América. Obligación establecida en el artículo 26 del Reglamento de la LPDP.

24.2. En el supuesto de resultar responsable, si debe aplicarse la exención de responsabilidad por la subsanación de la infracción, prevista en el literal f) del numeral 1 del artículo 257 de la LPAG, o las atenuantes, de acuerdo con lo dispuesto en el artículo 126 del reglamento de la LPDP.

24.3. Determinar en cada caso, la multa que corresponde imponer, tomando en consideración los criterios de graduación contemplados en el numeral 3) del artículo 248 de la LPAG.

V. Análisis de las cuestiones en discusión

Sobre el presunto tratamiento de datos personales sin haber obtenido válidamente el consentimiento para ello

25. El principio de consentimiento se tiene previsto en el artículo 5 de la LPDP:

> *"**Artículo 5. Principio de consentimiento***
> *Para el tratamiento de los datos personales debe mediar el consentimiento de su titular"*

26. Según lo dispone el inciso 13.5 del artículo 13 de la LPDP, los datos personales solo pueden ser objeto de tratamiento mediando el consentimiento del titular de los mismos, el mismo que deberá ser otorgado de manera previa, informada, expresa e inequívoca:

> ***"Artículo 13. Alcances sobre el tratamiento de datos personales***
> *(...)*
> *13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco."*

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

27. El numeral citado define entonces requisitos constitutivos del consentimiento, vale decir, los elementos sin los cuales no existe un consentimiento válidamente otorgado, conjuntamente con lo recogido en los artículos 11 y 12[16] del Reglamento de la LPDP,

[16] Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS
"Artículo 11.- Disposiciones generales sobre el consentimiento para el tratamiento de datos personales.
"El titular del banco de datos personales o quien resulte como responsable del tratamiento, deberá **obtener el consentimiento para el tratamiento de los datos personales, de conformidad con lo establecido en la Ley y en el presente reglamento** [...]
La solicitud del consentimiento deberá estar referida a un tratamiento o serie de tratamientos determinados, con expresa identificación de la finalidad o finalidades para las que se recaban los datos; **así como las demás condiciones que concurran en el tratamiento o tratamientos** [...].
Cuando se solicite el consentimiento para una forma de tratamiento que incluya o pueda incluir la transferencia nacional o internacional de los datos, el titular de los mismos deberá ser informado de forma que conozca inequívocamente tal

siendo tales requisitos de ser otorgado de forma previa, libre, expresa e inequívoca, y de manera informada.

28. Por otro lado, es preciso tener en cuenta que la obligación de obtener el consentimiento tiene excepciones, las cuales se encuentran previstas en el artículo 14 de la LPDP[17], no encontrándose inmerso en ninguno de ellas la administrada.

---

circunstancia, además de la finalidad a la que se destinarán sus datos y el tipo de actividad desarrollada por quien recibirá los mismos."
(el resaltado es nuestro)
Artículo 12.- Características del consentimiento.
Además de lo dispuesto en el artículo 18 de la Ley y en el artículo precedente del presente reglamento, la obtención del consentimiento debe ser:
1. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular de los datos personales. La entrega de obsequios o el otorgamiento de beneficios al titular de los datos personales con ocasión de su consentimiento no afectan la condición de libertad que tiene para otorgarlo, salvo en el caso de menores de edad, en los supuestos en que se admite su consentimiento, en que no se considerará libre el consentimiento otorgado mediando obsequios o beneficios. El condicionamiento de la prestación de un servicio, o la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios.
2. Previo: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron.
3. Expreso e Inequívoco: Con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron queda o pueda ser impreso en una superficie de papel o similar. La condición de expreso no se limita a la manifestación verbal o escrita. En sentido restrictivo y siempre de acuerdo con lo dispuesto por el artículo 7 del presente reglamento, se considerará consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie que ha consentido inequívocamente, dado que de lo contrario su conducta, necesariamente, hubiera sido otra.
Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer clic", "cliquear" o "pinchar", "dar un toque", "touch" o "pad" u otros similares. En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado. La sola conducta de expresar voluntad en cualquiera de las formas reguladas en el presente numeral no elimina, ni da por cumplidos, los otros requisitos del consentimiento referidos a la libertad, oportunidad e información.
4. Informado: Cuando al titular de los datos personales se le comunique clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente a. La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos. b. La finalidad o finalidades del tratamiento a las que sus datos serán sometidos. c. La identidad de los que son o pueden ser sus destinatarios, de ser el caso. d. La existencia del banco de datos personales en que se almacenarán, cuando corresponda. e. El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso. f. Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo. g. En su caso, la transferencia nacional e internacional de datos que se efectúen."

[17] **Artículo 14 de la LPDP:**
"Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.

29. De los hechos expuestos y analizados, la DPDP observa que la administrada realiza el servicio de gestión de venta telefónica (telemarketing) por encargo de GSP para la venta de productos (planes oncológicos) de Oncosalud; utilizando para ello una de las bases de datos de titularidad de la propia administrada denominada "Personas".

30. El contrato de prestación de servicios de abril 2010[18] (en adelante, el "Contrato"), suscrito entre Oncosalud S.A.C y la administrada, contempla en su Anexo 1 los servicios y condiciones para la venta de los planes de Oncosalud. En el numeral 14 de dicho Anexo 1 se estipula que para el desarrollo del servicio la administrada utilizará una base de datos propia, siendo responsable del contenido de la misma.

31. Con fecha 30 de junio de 2014, Oncosalud y la administrada suscribieron la Adenda N°3[19] al Contrato, por medio de la cual Oncosalud cede su posición contractual a favor de GSP e incluye un Anexo II al Contrato en el cual se estipula nuevamente que para el desarrollo del servicio la administrada utilizará su propia base de datos. En el numeral 15 de dicho Anexo II se estipula nuevamente que para el desarrollo del servicio la administrada utilizará una base de datos propia, siendo responsable del contenido de la misma:

> "***15. Base de Datos:*** *Para el desarrollo del servicio contratado,* ***SCC*** *utilizará una base de datos propia con la información de los prospectos a ser tomados en cuenta para la gestión comercial de venta de Planes de salud. Esta información deberá ser previamente remitida a* ***GSP*** *para ser filtrada por la lista de afiliados de la empresa.*
>
> *Así mismo,* ***SCC*** *es responsable por el contenido de la citada base de datos, debiendo filtrarla por el registro de consumidores "Gracias...no insista" de INDECOPI, entendiéndose que* ***SCC*** *asume la responsabilidad que pudiera generarse por una incorrecta actualización de la misma. Queda entendido que la propiedad de la citada base de datos corresponderá a* ***SCC****."* (El subrayado es nuestro)

32. Con fecha 28 de mayo de 2015, GSP y la administrada suscribieron la Adenda N°4[20] al Contrato, por medio de la cual incluyeron en el Contrato una cláusula adicional, referida a la protección y confidencialidad de datos respecto a los bancos de datos de titularidad de GSP a los cuales la administrada pueda acceder durante la ejecución del Contrato. En este sentido, las cláusulas 1.4 y 1.5 de la Adenda N°4 estipulan lo siguiente:

> *"1.4. Los bancos de datos se entenderán transferidos a dominio de GSP únicamente en lo referido a los datos personales de los clientes que adquieran los planes oncológicos que brinda la empresa ONCOSALUD S.A.C., y al momento de*

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ I

9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley".

[18] Folios 143 al 148
[19] Folios 176 al 177
[20] Folios 190 al 195

concretarse la afiliación, siempre y cuando el titular de los datos haya otorgado su autorización para ello.

1.5. Los datos personales de aquellas personas que hayan sido contactados por EL PROVEEDOR y que no hayan sido afiliados como clientes de GSP y/o a ninguno de los planes ofrecidos materia del presente contrato, serán descartados y eliminados de manera automática de todo registro que esté bajo dominio de EL PROVEEDOR, dentro de las 24 horas de realizada la llamada, sin que se genere para ello una base de datos de ningún tipo. Así, EL PROVEEDOR declara que no creará, tratará o administrará ningún banco de datos que contenga los datos personales de aquellas personas descartadas como clientes y/o usuarios de los productos y/o servicios ofrecidos por GSP."

33. Del Contrato se desprende claramente que el servicio de gestión de ventas de los planes oncológicos de Oncosalud será realizado por la administrada para lo cual deberá utilizar su propia base y/o banco de datos con información de prospectos de clientes, siendo responsable por el contenido de la misma. También resulta responsable del tratamiento de aquellos datos incluidos en los bancos de datos de titularidad de GSP a los que la administrada pueda haber tenido acceso: (i) en caso de afiliaciones dichos datos serán transferidos a GSP formando parte del banco de datos de clientes de titularidad de esta última, y (ii) de no concretarse una afiliación, los datos de la persona contactada deberán ser eliminados de todo registro de la administrada, prohibiéndose la generación y alimentación de un banco de datos que contenga dicha información.

34. En el presente caso, se aprecia que la administrada es titular de seis (6) bancos de datos personales debidamente inscritos ante el Registro Nacional de Protección de Datos Personales (en adelante, el "RNPDP"), denominados i) "Colaboradores", ii) "Personas", iii) "Reclutamiento", iv) "Control de Acceso Físico", v) "Videovigilancia" y vi) Clientes.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ

35. Para efectos de análisis, es pertinente considerar la información declarada y registrada del banco de datos "Personas", inscrito con código RNPDP-PJP N° 2779 en el RNPDP. Dicho banco de datos fue inscrito mediante Resolución Directoral N° 759-2015-JUS/DGPDP-DRN de fecha 17 de junio de 2015, el mismo que fue modificado por Resolución Directoral N° 2287-2016-JUS/DGPDP-DRN de fecha 6 de setiembre de 2016.

36. El banco de datos "Personas" declarado por la administrada al RNPDP registra la siguiente información:

Código:	RNPDP-PJP N°2779
Denominación:	PERSONAS
Finalidad:	Buscar números actualizados de posibles clientes para realizar llamadas telefónicas
Usos previstos:	Gestión de listas de clientes; análisis de perfiles; fines estadísticos, históricos o científicos.
Tipos de datos personales:	Datos de características personales: N° de DNI, teléfono
Procedimientos de obtención:	Fuente: Del titular del dato personal o su representante legal Soporte: Informático/magnético, vía telemática. Procedimiento: Transmisión electrónica, proveedores de datos personales y números telefónicos
Sistema de tratamiento:	Automatizado
Medidas de seguridad:	Indica que cuenta con un documento de seguridad.
Receptores de los datos personales a nivel nacional:	Indica que realiza transferencia de datos a organizaciones o personas directamente relacionadas.

PERU Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

37. Como se puede apreciar, dentro de los procedimientos de obtención de la información contenida en la base de datos "Personas" se contemplan la transmisión electrónica, proveedores de datos personales y números telefónicos. Asimismo, se establece como finalidad la búsqueda de números de posibles clientes para la realización de llamadas.

38. El personal de fiscalización verificó que el tratamiento de la base de datos "Prospecto de Clientes" es realizado en soporte automatizado por tiempo indeterminado a través de los sistemas MOVE IT, CRM, SICCAB (CRM) y el aplicativo Microsoft Excel.

39. Según las diversas constataciones realizadas por el personal fiscalizador, se ha evidenciado que la administrada alimenta el banco de datos "Personas" con la información remitida por Infocore (números de DNI y números telefónicos). Infocore remite dicha información a la administrada mediante el aplicativo (sistema) MOVE IT, en virtud de un contrato de transferencia de datos que tiene suscrito con la administrada.

40. Según el Contrato de Transferencia de Datos y Página web de consultas de fecha 1 de mayo de 2017, suscrito entre la administrada e Infocore (en adelante, el "Contrato de Transferencia de Datos[21]") esta última transfiere registros de datos (números telefónicos) y en general todo registro que brinda los servicios de Infocore.

41. En la cuarta visita de fiscalización, se verificó que la información del banco de datos de titularidad de la administrada utilizada para la venta de seguros oncológicos de Oncosalud, es obtenida a través del sistema web de importación de datos Infocore. Se verificó que, para la obtención de los números telefónicos, la administrada debe ingresar

[21] Folios 43 al 49

a la web de importación de datos de Infocore los números de DNI para que a su vez el sistema le arroje los números telefónicos que estén asociados a estos últimos. Según manifestación de la administrada, los números de DNI son descargados previamente por ella a través del enlace http://dniperu.online/.

42. Del documento "Proceso de obtención de información a través del Sistema de Importación de Datos INFOCORE"[22] entregado por la administrada en la cuarta visita de fiscalización, se detalla, lo siguiente:

- Infocore proporciona una cuenta de usuario y contraseña para el ingreso a su sistema web de importación de datos.
- Primero, la administrada ingresa a páginas públicas como Páginas Blancas para buscar nombres y apellidos.
- Segundo, la administrada entra al enlace http://dniperu.online/ donde ingresa manualmente los nombres y apellidos extraídos previamente para así obtener los números de DNI.
- Tercero, la administrada ingresa los números de DNI al sistema web de importación de datos de Infocore.
- Cuarto, el sistema web de Infocore permite descargar a la administrada los números telefónicos asociados a los DNIs.

43. De los hechos expuestos, este Despacho aprecia que la administrada recopila los datos personales constituidos por nombres y apellidos, así como números de DNIs sin el consentimiento válido de sus titulares para a su vez transferirlos a un tercero (Infocore) para la obtención de sus números telefónicos y así, finalmente, generar y alimentar su banco de datos "Personas". Este banco de datos "Personas" contiene la lista de prospecto de clientes a los cuales la administrada ofrecerá los productos de Oncosalud en virtud de la obligación contractual que sostiene con GSP.

44. Respecto a la generación del banco de datos personales "Personas" de titularidad de la administrada, este Despacho considera relevante pronunciarse sobre si el tratamiento de los datos contenidos en dicho banco de datos resulta acorde o no con la normativa de protección de datos personales, partiendo para ello del análisis de la necesidad de contar con el consentimiento libre, inequívoco, previo, expreso e informado de sus titulares.

PERU Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

45. De la información contenida en el expediente materia de análisis, se desprende que la generación de estos registros provienen de información extraída por la administrada de (i) Páginas Blancas (obtención de nombres y apellidos), (ii) el enlace http://dniperu.online/ (obtención de números de DNIs) y (iii) del sistema web de importación de datos de Infocore (obtención de números telefónicos).

46. El artículo 2, numeral 4, de la LPDP define como dato personal a *"toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados"*. Complementariamente, el artículo 4, numeral 4, del Reglamento de la LPDP define como dato personal a *"aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados"*.

47. La DPDP no es ajena al desarrollo tecnológico que permite que herramientas virtuales como la navegación y búsqueda por Internet que pueden poner a disposición

[22] Folios 230 al 234

del internauta enlaces como http://dniperu.online/, así como la digitalización de las fuentes accesibles al público como directorios/guías telefónicas de donde la administrada recopila información para alimentar su banco de datos.

48. En este orden de ideas, es oportuno recalcar que los datos contenidos en las fuentes de acceso al público deben emplearse únicamente para el propósito para el cual dicha fuente fue creada y, por ende, coloca a disposición dicha información. Esto es, para el caso de los directorios o guías telefónicas que contengan información de abonados, para uso personal y/o doméstico en el supuesto de necesidad de contactarlo previo conocimiento de la persona por parte del interlocutor. Para el caso de las búsquedas en RENIEC, por ejemplo, para verificar la identidad de personas y evitar suplantaciones. Las búsquedas en SUNAT, para corroborar si una persona natural cuenta con negocio propio o qué tipo de actividad económica desarrolla, ello en virtud de una relación contractual, por citar un ejemplo. Para el caso de los medios de navegación y búsqueda por Internet, para uso meramente informativo sin que esto implique una habilitación descontrolada al internauta para la difusión o transferencia de los datos personales que pueda recoger de la Web para fines distintos a su uso doméstico o de carácter informativo (como en el presente caso, obtener un número telefónico para finalidades comerciales).

49. En ningún caso la información que fuera recopilada de fuentes de acceso al público como las aquí mencionadas facultan al usuario de las mismas a incorporarlas en bancos de datos para un tratamiento que no hubiera sido consentido válidamente conforme lo establecido en la normativa de protección de datos personales.

50. Para un tratamiento que tiene una finalidad distinta a la cual causó la creación de dicha fuente, deberá obtenerse el consentimiento válido de cada titular, tal como en su momento detalló la Dirección General de Transparencia, Acceso a la Información Pública a través del Oficio N° 749-2018-JUS/DGTAIPD del 7 de agosto de 2018: *"(...) los datos contenidos en las fuentes de acceso al público deben de utilizarse únicamente dentro del marco para el cual dicha fuente ha sido creada y pone a disposición la información mencionada. (...) En caso se requiera realizar tratamientos para finalidades distintas a aquellas para las cuales los datos personales fueron puestos a disposición en las fuentes accesibles al público, como por ejemplo remitir publicidad, deberá solicitarse el consentimiento conforme al artículo 5 y el artículo 13, inciso 13.5 de la LPDP"*

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

51. El principio de finalidad consiste en que los datos personales deben ser recopilados para una finalidad determinada, siendo que el tratamiento de dichos datos de ninguna manera puede ser extendido a una finalidad distinta a la cual haya sido autorizada al momento de su recopilación del titular. En este sentido, el artículo 6 de la LPDP, desarrolla el concepto de dicho principio:

> ***"Artículo 6. Principio de finalidad***
> *Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización."*

52. Adicionalmente, el artículo 8 del Reglamento de la LPDP complementa esta definición señalando que *"una finalidad está determinada cuando haya sido expresada*

con claridad, sin lugar a confusión y cuando de manera objetiva se especifica el objeto que tendrá el tratamiento de los datos personales".

53. En el presente caso, se observa que la información recabada y contenida en la base de datos "Personas" de titularidad de la administrada obedece a una finalidad totalmente distinta a aquellas vinculadas al uso de las propias fuentes de acceso público de las cuales son extraídos los datos personales. La finalidad del banco de datos "Personas" declarada por la administrada al RNPDP, es la búsqueda de números de posibles clientes para la realización de llamadas. Siendo que esta finalidad se aleja del propósito de las fuentes de acceso público para el cual se autoriza un tratamiento sin consentimiento previo de los titulares de los datos personales a los cuales se accede, resulta estrictamente necesario que la administrada procure y obtenga el consentimiento válido de cada uno de los titulares cuyos datos personales incorpore en la base de datos "Personas", orientando sobre los usos previstos y finalidad de dicho banco de datos, la cual -conforme se desprende del presente caso- gira en torno al ofrecimiento de productos y/o servicios de sus clientes, siendo uno de ellos GSP (para la gestión de venta de los planes oncológicos de Oncosalud)

54. Este Despacho considera pertinente resaltar que la obligación de obtener el consentimiento previo no implica una prohibición absoluta de contacto, toda vez que dicha prohibición imposibilitaría justamente el hecho generador del consentimiento y/o autorización que se busca obtener. No obstante ello, la administrada no ha presentado prueba alguna que acredite la obtención del consentimiento de los titulares de los datos personales para el almacenamiento de sus datos en el banco de datos "Personas" con fines comerciales.

55. Respecto a este primer hecho infractor imputado, la administrada ha señalado en sus descargos que el Contrato de Transferencia de Datos fue resuelto por mutuo disenso con anterioridad a la notificación del inicio del procedimiento sancionador. La administrada acotó que suscribió un nuevo contrato con Infocore, señalando que en virtud del mismo ya no remiten base de datos con nombres y DNIs a Infocore para la obtención de números telefónicos asociados a tales datos, sino que Infocore queda obligado a transferir únicamente números telefónicos (celulares y fijos) no relacionados, obtenidos de fuentes de acceso al público. La administrada adjuntó a sus descargos presentados el 24 de abril de 2019 (i) el Acuerdo de Resolución por Mutuo Disenso[23] suscrito con Infocore de fecha 28 de febrero de 2019 (en adelante, el "Acuerdo de Muto Disenso") y (ii) el Contrato de Transferencia de Datos[24] de fecha 1 de marzo de 2019 (en adelante, el "Nuevo Contrato de Transferencia de Datos").

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ I

56. Acerca de la supuesta anterioridad de dicho documento respecto del inicio de este procedimiento sancionador, al datar supuestamente de 1 de marzo de 2019, debe tenerse en cuenta lo establecido en el considerando 21 de esta Resolución Directoral, en el que se detalla lo previsto en el literal f) del numeral 1 del artículo 257 de la LPAG, y que para su aplicación, se requiere que el documento de seguridad mencionado, tenga una fecha cierta previa a la notificación de imputación de cargos (realizada el 1 de abril de 2019, con la notificación a la administrada de la Resolución Directoral N° 040-2019-JUS/DGTAIPD-DFI).

57. Un documento adquiere fecha cierta en los siguientes supuestos previstos en el Código Procesal Civil:

"Artículo 245.- Fecha cierta. -

[23] Folios 450 al 451
[24] Folios 452 al 459

> *Un documento privado adquiere fecha cierta y produce eficacia jurídica como tal en el proceso desde:*
> *1.- La muerte del otorgante.*
> *2.- La presentación del documento ante funcionario público.*
> *3.- La presentación del documento ante notario público, para que certifique la fecha o legalice las firmas.*
> *4.- La difusión a través de un medio público de fecha determinada o determinable.*
> *5.- Otros casos análogos.*
> *Excepcionalmente, el Juez puede considerar como fecha cierta la que haya sido determinada por medios técnicos que le produzcan convicción."*
> (El subrayado es nuestro)

58. Al carecer de certificación de fecha o legalización de firmas o de difusión en fecha determinable, la única fecha que puede considerarse como cierta para el documento de seguridad es la de su presentación en mesa de partes, esto es el 24 de abril de 2019.

59. Para contar con el respaldo del principio de Presunción de Veracidad, es necesario que la información declarada cumpla el requisito establecido en el artículo 67 de la LPAG, en los siguientes términos:

> ***"Artículo 67.- Deberes generales de los administrados en el procedimiento***
> *Los administrados respecto del procedimiento administrativo, así como quienes participen en él, tienen los siguientes deberes generales:*
> *(...)*
> *4. Comprobar previamente a su presentación ante la entidad, la autenticidad de la documentación sucedánea y de cualquier otra información que se ampare en la presunción de veracidad."*

Este deber supone ser ejercido bajo los principios de la buena fe y colaboración procedimental que son en torno a los cuales deben conducirse las partes dentro de un procedimiento administrativo sancionador como, en el presente caso, al momento de ofrecer pruebas.

60. Los administrados no deben ampararse indiscriminadamente en el principio de Presunción de Veracidad para encubrir situaciones que de haberse inclusive configurado en la realidad hayan sido materializadas, posteriormente, a la imputación de cargos para buscar ser consideradas como acciones de subsanación. Para evitarse un aprovechamiento indebido de este principio, la Autoridad Administrativa exige la acreditación de la autenticidad de la información y documentación presentada por parte del administrado. En el caso materia de pronunciamiento, resulta razonable exigir la acreditación de fecha cierta del Nuevo Contrato de Transferencia, dado que estando dentro de un procedimiento sancionador, en el cual la administrada ha tenido hasta seis fiscalizaciones y ha sido notificada correctamente del Informe de Fiscalización N°004-2019-JUS/DGTAIPD-DFI-AARM con fecha 28 de enero de 2019, pudo haber actuado diligentemente y certificar la fecha de suscripción del contrato por notario público o inclusive haberlo presentado junto a sus primeros descargos del 1 de marzo de 2019, lo cual no hizo. Por lo expuesto, este Despacho concluye que solo se puede tener como fecha cierta del documento, la fecha de presentación del mismo en mesa de partes, siendo que en caso se presenten las acciones de corrección, estas son evaluadas como acciones de enmienda dirigidas a atenuar la responsabilidad administrativa, mas no de subsanación de la conducta infractora que la eximan de responsabilidad alguna.

61. Sin embargo, en este caso, no se ha subsanado la imputación referida al tratamiento de datos sin consentimiento, puesto que si bien ya no recibían los números

telefónicos asociados a nombres y números de DNI; es preciso señalar que los números de teléfonos por sí solos constituyen datos personales puesto que hacen identificable al titular del dato personal.

62. Al respecto, la Autoridad Nacional de Protección de Datos Personales, mediante la Opinión Consultiva N° 26-2019-JUS/DGTAIPD, ha señalado lo siguiente:

"4. Un número de teléfono celular que no está vinculado a un dato adicional que dé indicios de la identidad de una persona es un dato personal[25], puesto que, si bien dicho número por sí solo no identifica a la persona, sí la hace identificable.

5. Al respecto, la Ley N° 29733, Ley de Protección de Datos Personales(LPDP), artículo 2, numeral 4, define como dato personal a "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

6. De forma complementaria, el Reglamento de la LPDP, aprobado mediante el Decreto Supremo 003-2013-JUS, artículo 4, numeral 4, desarrolla la definición de datos personal, señalando que "es aquella información numérica, alfabética, grafica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados".

7. En este caso, dado que en internet se encuentran publicados directorios de teléfonos celulares, un número de teléfono celular que se almacena sin vincularlo a otro dato personal que identifique a una persona determinada, sí es un dato personal, ya que dicho número hace la identificable mediante medios que pueden ser razonablemente utilizados; como por ejemplo, mediante la revisión de directorios publicados en internet.

8. En esa misma línea, un número generado a partir de la combinación aleatoria de nueve dígitos es un dato personal si corresponde a un número de teléfono celular o a algún dato que identifique o haga identificable a una persona."

63. Por lo tanto, la medida tomada por la administrada, respecto a obtener los números telefónicos sin asociarlos a un nombre en un primer momento, no constituye acción de enmienda respecto a la imputación realizada.

64. Esta Dirección considera que existen pruebas suficientes para concluir que la administrada ha recabado y hecho tratamiento de datos personales contenidos en su banco de datos "Personas", que utiliza como base de datos de prospección de clientes, para la venta de los planes oncológicos de Oncosalud en virtud del Contrato suscrito con GSP, sin el consentimiento válido de los titulares de dichos datos. La administrada ha declarado e inscrito su base de datos, bajo código RNPDP-PJP N° 2779, en el RNPDP en junio de 2015 (según se menciona en el considerando 35 de la presente Resolución Directoral) y, sin embargo, no ha presentado ningún medio probatorio que acredite que hubiere recabado el consentimiento válido de los titulares de los datos registrados en dicho banco a partir de dicho mes en adelante.

[25]La LPDP define, en el artículo 2, numeral 4, al dato personal como "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

65. El artículo 15[26] del Reglamento de la LPDP establece que la carga de la prueba sobre la obtención del consentimiento recae exclusivamente en el titular del banco de datos personales, en este caso, en la administrada. Según lo expuesto a lo largo de la presente Resolución Directoral, se concluye que la administrada no ha probado haber obtenido el consentimiento válido de los titulares de los datos personales contenidos en su banco de datos "Personas. Conforme ha sido evidenciado, y manifestado por la misma administrada, esta última ha realizado tratamiento deliberado y no autorizado de datos personales (búsqueda, importación y transferencia) como los nombres, apellidos y números de DNIs de diversas personas para seguidamente transferirlos a Infocore para que a su vez este último realice tratamiento de los mismos y le envíe números telefónicos asociados a dichos datos a cambio de una contraprestación.

66. En este orden de ideas, la administrada estaba obligada a contar con el consentimiento válido de los titulares de los datos personales almacenados en su base de datos "Personas", de forma previa a efectuar las llamadas por encargo de GSP y Oncosalud, lo cual no ha demostrado en el presente procedimiento sancionador. La administrada ni siquiera ha presentado prueba fehaciente de que a partir de la ejecución del Nuevo Contrato de Transferencia cumpla con obtener el consentimiento válido de los titulares de los números telefónicos con los cuales realiza el primer contacto para el tratamiento de sus datos personales para el ofrecimiento comercial de productos y/o servicios de sus diversos clientes corporativos en virtud de las gestiones de telemarketing y contact center que les brinda.

67. De una revisión del Acuerdo de Muto Disenso y del Nuevo Contrato de Transferencia de Datos, se desprende que el objeto de los mismos es limitar la responsabilidad de las partes, en tanto la administrada ya no transferirá nombres, apellidos y números de DNIs a Infocore para la provisión de números telefónicos y esta última transferirá números telefónicos obtenidos de fuentes de acceso público en observancia de la normativa de protección de datos personales (conforme a lo estipulado en la cláusula novena del Nuevo Contrato de Transferencia de Datos). No obstante ello, conforme a lo desarrollado a partir del considerando 48 de la presente Resolución Directoral, este Despacho insiste en remarcar que no basta ampararse en la obtención e importación de datos personales de fuentes de acceso público para darles un tratamiento distinto a la finalidad de uso de dicha fuente, las cuales son ajenas a la comercialización de dichos datos de no existir consentimiento válido y previamente informado de sus titulares.

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

68. La LPDP establece en el numeral 9 de su artículo 13 que *"La comercialización de datos personales contenidos o destinados a ser contenidos en bancos de datos personales se sujeta a los principios previstos en la presente Ley"*. Si bien la misma ley no prohíbe el servicio de comercialización de datos por transferencia de los mismos, como lo es el caso del servicio brindado por Infocore, ello debe ser enmarcado dentro del ámbito de la ley, en observancia del principio rector del consentimiento. Es menester aclarar que la infracción imputada se configura por no contar con el consentimiento válido de los titulares para realizar el tratamiento de sus datos personales (importarlos deliberadamente para fines distintos a los intrínsecamente vinculados a cada fuente accesible al público, transferirlos a un tercero para obtener otro dato personal asociado, almacenarlos en su banco de datos para, finalmente, destinarlos a fines comerciales).

---

[26] Artículo 15 del Reglamento de la LPDP:
"Artículo 15.- Consentimiento y carga de la prueba.
Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley y en el presente reglamento, la carga de la prueba recaerá en todos los casos en el titular del banco de datos personales o quien resulte el responsable del tratamiento."

69. Respecto a la evaluación de si la administrada ha implementado alguna acción de enmienda necesaria para la atenuación de la responsabilidad administrativa prevista en el artículo 126 del Reglamento de la LPDP, este Despacho considera que la administrada no ha ejecutado ninguna acción de enmienda. El hecho de que la administrada haya presentado y referido su Nuevo Contrato de Transferencia de Datos no resulta suficiente, en tanto no ha acreditado que ejecuta mecanismos válidos para la obtención del consentimiento de los titulares para el registro de sus datos personales en su base de datos "Personas". La sola presentación de dicho documento, así como el documento de "Resolución por Mutuo Disenso" no acredita para este Despacho que la administrada haya obtenido válidamente el consentimiento de los titulares de datos personales que contiene su banco de datos.

70. Sobre la alusión hecha por la administrada a un pronunciamiento previo de la DPDP, donde se impuso una sanción de multa de 5.5UIT por la comisión de una infracción grave, considerándose que no existe un perjuicio económico causado y reincidencia por parte del administrado, como ocurre en el presente caso; este Despacho advierte una inferencia errada. En primer lugar, se trata de imputación de cargos distintos, ya que en el referente de la administrada se imputó una conducta de recopilación de datos vía sitio web sin facilitar las políticas de privacidad con la información establecida en el artículo 18 de la LPDP, siendo que el nivel de incumplimiento a criterio de la DPDP no fue tan alto, considerando que hubo acciones de mejora y de enmienda que fueron tomadas en cuenta. En segundo lugar, se trata de situaciones de recopilación totalmente diferentes, siendo que en el caso referido por la administrada es el mismo titular quien pone a disposición del administrado sus datos personales, a diferencia de la administrada quien realiza tratamiento indebido de los mismos desde que los recopila, transfiere a un tercero y almacena sin contar con el consentimiento de sus titulares. En tercer lugar, el que no exista un perjuicio económico causado ni reincidencia son parte de los criterios generales que se toman en cuenta para imponer y motivar una sanción, no los únicos, puesto que deben ser evaluados de forma contextual, considerando la magnitud del hecho infractor. El que no se advierta perjuicio económico causado no implica que no se haya vulnerado la protección de los datos personales de sus titulares, en tanto la administrada está haciendo uso indebido de los mismos. Y, finalmente, si no se advierte reincidencia, esto se traduce en que es la primera vez que se detecta el hecho infractor.

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

71. Por lo expuesto, la administrada es responsable por la comisión de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP.

Sobre el presunto incumplimiento de inscripción en el RNPDP del banco de datos personales de usuarios del sitio web de la administrada

72. Este Despacho, concuerda con la DFI en considerar como eximentes de responsabilidad que el hecho de que los bancos de datos "Colaboradores" y "Reclutamiento" de titularidad de la administrada almacenen datos personales recopilados a través de los enlaces del sitio web www.scc.com.pe de titularidad de la administrada "Buzón de Propuestas" e "Ingresa tu CV", respectivamente. Ello en tanto, ambos bancos de datos fueron inscritos en el RNPDP en el año 2015 y 2016, respectivamente.

73. Sin embargo, respecto al banco de datos "Clientes" que contiene datos personales recopilados a través del enlace del sitio web www.scc.com.pe "Ponte en Contacto", este Despacho considera que la presentación de la solicitud de inscripción con fecha de 7 de

febrero de 2019 (previo a la notificación del inicio del procedimiento sancionador) debe ser tomada como un eximente de responsabilidad a favor de la administrada.

74. Por lo expuesto, la administrada no es responsable por la comisión de la infracción grave tipificada en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP.

Sobre el presunto incumplimiento de comunicación de flujo transfronterizo que realiza de los datos personales de usuarios del sitio web de la administrada

75. Este Despacho, concuerda con la DFI en considerar como eximente de responsabilidad el hecho de que el banco de datos "Colaboradores" cuenta con inscripción de la comunicación de que realiza flujo transfronterizo antes del inicio del procedimiento administrativo sancionador, en tanto ello fue realizado agosto de 2018, según consta en la Resolución Directoral N° 1852-2018-JUS/DGTAIPD-DPD del 8 de agosto de 2018.

76. Sin embargo, respecto al banco de datos "Reclutamiento" y "Clientes", este Despacho considera que la presentación de ambas solicitudes de inscripción de comunicación de flujo transfronterizo con fecha de 7 de febrero de 2019 (previo a la notificación del inicio del procedimiento sancionador) deben ser tomadas como un eximente de responsabilidad a favor de la administrada.

77. Por lo expuesto, la administrada no es responsable por la comisión de la infracción grave tipificada en el literal e) del numeral 1 del artículo 132 del Reglamento de la LPDP.

Sobre las sanciones a aplicar a los hechos analizados

78. La Tercera Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1353, modificó el artículo 38 de la LPDP que tipificaba las infracciones a la LPDP y su reglamento, incorporando el artículo 132 al Título VI sobre Infracciones y Sanciones de dicho reglamento, que en adelante tipifica las infracciones.

79. Por su parte, el artículo 39 de la LPDP establece las sanciones administrativas calificándolas como leves, graves o muy graves y su imposición va desde una multa de cero coma cinco (0,5) unidades impositivas tributarias hasta una multa de cien (100) unidades impositivas tributarias[27], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[28].

PERÚ | Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

[27] **Ley N° 29733, Ley de Proteccion de Datos Personales**
"**Artículo 39. Sanciones administrativas**
En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:
1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).
2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).
3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT)."

[28] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"Artículo 118.- Medidas cautelares y correctivas.
Una vez iniciado el procedimiento sancionador, la Dirección de Sanciones podrá disponer, mediante acto motivado, la adopción de medidas de carácter provisional que aseguren la eficacia de la resolución final que pudiera recaer en el referido procedimiento, con observancia de las normas aplicables de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
Asimismo, sin perjuicio de la sanción administrativa que corresponda por una infracción a las disposiciones contenidas en la Ley y el presente reglamento, se podrán dictar, cuando sea posible, medidas correctivas destinadas a eliminar, evitar o detener los efectos de las infracciones."

80. En el presente caso, se ha establecido la responsabilidad de la administrada por lo siguiente:

- No contar con el consentimiento de los titulares de los datos personales almacenados en el banco de datos personales de titularidad de la administrada denominado "Personas" para recopilarlos y usarlos para la gestión de venta telefónica (telemarketing), de acuerdo con el numeral 13.5 del artículo 13 de la LPDP y el artículo 12 del Reglamento de la LPDP, configurando la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 de dicho reglamento; conducta sancionable con una multa de entre cinco (5) y cincuenta (50) unidades impositivas tributarias, de acuerdo con lo establecido en el artículo 39 de dicha ley.

81. Cabe señalar que esta dirección determina el monto de las multas a ser impuestas tomando en cuenta para su graduación los criterios establecidos en el numeral 3 del artículo 248 de la LPAG. En tal sentido, debe prever que la comisión de las conductas sancionables no resulte más ventajosa para el infractor que cumplir las normas infringidas o asumir la sanción administrativa, por lo que la sanción deberá ser proporcional al incumplimiento calificado como infracción, observando para ello los criterios que dicha disposición señala para su graduación.

82. En el presente caso, se considera como criterios relevantes para graduar las sanciones, los siguientes:

a) <u>El beneficio ilícito resultante por la comisión de las infracciones:</u>

Se ha evidenciado el beneficio ilícito a favor de la administrada, resultante de la comisión de la infracción cometida, considerando que utiliza los datos contenidos en su base "Personas" con fines comerciales, sin haber informado debidamente a los titulares de dichos datos las condiciones del tratamiento de sus datos para la obtención de su consentimiento válido.

PERU Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

b) <u>La probabilidad de detección de las infracciones:</u>

Al haberse configurado el hecho infractor por medio de generación y alimentación de la base de datos "Personas" sin consentimiento de sus titulares, resulta que la posibilidad de detección sea baja en tanto que ha sido necesario efectuar visitas de fiscalización para su detección.

c) <u>La gravedad del daño al interés público y/o bien jurídico protegido:</u>

Las infracciones detectadas afectan el derecho fundamental a la protección de datos personales, el cual se encuentra reconocido en el artículo 2, numeral 6, de la Constitución Política del Perú, siendo desarrollado por la LPDP y su reglamento.

Acerca del incumplimiento del inciso 13.5 del artículo 13 de la LPDP, debe señalarse que implica la vulneración de uno de los principios del tratamiento de datos personales, como es el principio de Consentimiento, lo que implica atentar contra la autodeterminación informativa de la persona, al no permitírsele decidir sobre el destino y acciones a efectuar con sus datos personales con la debida información para tomar tal decisión, incumpliendo con uno de los principales elementos legitimadores del tratamiento de datos personales de terceros.

d) El perjuicio económico causado:

No se evidencia un perjuicio económico resultante de la comisión de las infracciones.

e) La reincidencia en la comisión de las infracciones:

La administrada no fue sancionada anteriormente por la infracción detectada.

f) Las circunstancias de la comisión de la infracción:

La administrada en ningún momento a lo largo del presente procedimiento ha evidenciado que ha implementado mecanismos efectivos ni acciones de enmienda para la obtención del consentimiento y regularizar el tratamiento indebido que realiza de los datos personales contenidos en su base de datos "Personas".

g) La existencia o no de intencionalidad en la conducta del infractor:

Ha quedado probada la responsabilidad de la administrada en la comisión de la infracción imputada, no habiéndose advertido por este Despacho acción de enmienda efectiva y probada respecto a la situación infractora.

83. Es pertinente indicar que para imponer la sanción se tendrá en cuenta la suma de todos los hechos analizados en la presente Resolución Directoral.

84. De otro lado, es pertinente tomar en consideración lo que se aprecia en la Declaración Jurada Anual de Rentas de la administrada, correspondiente al ejercicio fiscal 2018, en la que se aprecia que, como ingreso bruto, obtiene S/. 43,993,655, siendo el límite para la imposición de multa el 10% de dicho concepto (S/.4, 399,365.5).

Por las consideraciones expuestas y de conformidad con lo dispuesto por la LPDP y su reglamento, la LPAG, y el Reglamento del Decreto Legislativo N° 1353;

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección de Protección de Datos Personales
M. GONZALEZ L.

SE RESUELVE:

Artículo 1.- Sancionar a SERVICIOS DE CALL CENTER DEL PERÚ S.A., con la multa ascendente a veinticinco unidades impositivas tributarias (25 UIT) por la comisión de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP: *"Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley N° 29733 y su Reglamento"*.

Artículo 2.- Imponer como medidas correctivas a SERVICIOS DE CALL CENTER DEL PERÚ S.A., lo siguiente:

- Obtener el consentimiento de los titulares de los datos personales que almacena en el banco de datos "Personas" para gestiones comerciales, y eliminar los datos personales de aquellos titulares de datos personales almacenados en dicho banco que no le otorguen el consentimiento conforme la LPDP.

Para el cumplimiento de tal medida correctiva, se otorga el plazo de treinta (30) días hábiles contados a partir de la notificación que declare consentida o firme la presente resolución directoral.

Artículo 3.- Informar a SERVICIOS DE CALL CENTER DEL PERÚ S.A., que el incumplimiento de la medida correctiva señalada constituye la comisión de la infracción tipificada como muy grave en el literal d) del numeral 3 del artículo 132 del Reglamento de la LPDP[29].

Articulo 4.- Informar a SERVICIOS DE CALL CENTER DEL PERÚ S.A, que contra la presente resolución, de acuerdo con lo indicado en el artículo 218 de la LPAG, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación[30].

Artículo 5.- Informar a SERVICIOS DE CALL CENTER DEL PERÚ S.A, que el pago de la multa será requerido una vez que la resolución que impone la sanción quede firme. En el requerimiento de pago se le otorgará diez (10) días hábiles para realizarlo y se entenderá que cumplió con pagar la multa impuesta, si antes de que venza el plazo mencionado, cancela el sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP[31].

Artículo 6.- Notificar a SERVICIOS DE CALL CENTER DEL PERÚ S.A la presente resolución.

Regístrese y comuníquese.

MARÍA ALEJANDRA GONZÁLEZ LUNA
Directora (e) de la Dirección de Protección de Datos Personales
Ministerio de Justicia y Derechos Humanos

---

[29] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS**
"TÍTULO VI INFRACCIONES Y SANCIONES
CAPÍTULO IV
INFRACCIONES
Artículo 132.- Infracciones
Las infracciones a la Ley N° 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.
(...)
3.Son infracciones muy graves:
(...)

d) No cesar en el indebido tratamiento de datos personales cuando existiese un previo requerimiento de la Autoridad como resultado de un procedimiento sancionador o de un procedimiento trilateral de tutela."

[30] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS**
"**Artículo 218. Recursos administrativos**
218.1 Los recursos administrativos son:
a) Recurso de reconsideración
b) Recurso de apelación
Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.
218.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días."

[31] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS**
"Artículo 128.- Incentivos para el pago de la sanción de multa.
Se considerará que el sancionado ha cumplido con pagar la sanción de multa si, antes de vencer el plazo otorgado para pagar la multa, deposita en la cuenta bancaria determinada por la Dirección General de Protección de Datos Personales el sesenta por ciento (60%) de su monto. Para que surta efecto dicho beneficio deberá comunicar tal hecho a la Dirección General de Protección de Datos Personales, adjuntando el comprobante del depósito bancario correspondiente. Luego de dicho plazo, el pago sólo será admitido por el íntegro de la multa impuesta."