Resolución Directoral N° 1797 -2021-JUS/DGTAIPD-DPDP

Expediente N°
106-2019-JUS/DGTAIPD-PAS

Lima, 07 de julio de 2021

VISTOS:

El Informe Nº 153-2019-JUS/DGTAIPD-DFI del 29 de noviembre de 2019[1], 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"), junto con los demás documentos que obran en el respectivo expediente; la Resolución Directoral 12-2021-JUS/DGTAIPD y,

CONSIDERANDO:

I. Antecedentes

1. Mediante la Orden de Visita de Fiscalización Nº 01-2019-JUS/DGTAIPD-DFI[2] de fecha 7 de enero de 2019, la DFI dispuso iniciar actividad de fiscalización a SENTINEL PERÚ S.A., identificada con R.U.C. N°20525138985, (en adelante, la "administrada"), a fin de determinar si dicha entidad, en el desarrollo de sus actividades, cumple con las disposiciones 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"), respecto a la transferencia de datos personales de contacto (números telefónicos y direcciones domiciliarias) a Caja Municipal de Ahorro y Crédito de Piura S.A.C (en adelante, "CMAC Piura". Ello en atención de la recomendación determinada en el Informe Final de Fiscalización N° 191-2018-JUS/DGTAIPD-DFI-AAR[3]

2. Con fecha 7 de enero de 2019, se realizó la primera visita de fiscalización, dejándose constancia de lo verificado en el Acta de Fiscalización N° 01-2019[4].

3. Con fecha 14 de enero de 2019, se realizó la segunda visita de fiscalización, dejándose constancia de los hechos en el Acta de Fiscalización N° 02-2019[5].

[1] Folios 206 a 215
[2] Folio 8
[3] Folios 1 a 6
[4] Folios 9 a 41
[5] Folios 54 a 70

4. Mediante Oficio N° 364-2019-JUS/DGTAIPD-DFI, notificado el 02 de mayo de 2019[6], la DFI requiere a la administrada que presente lo siguiente:

De la muestra tomada de veintidós (22) registros que figuran en el archivo Excel remitido por SENTINEL PERU S.A. a CMAC Piura el 6 de agosto de 2018, que consta en el documento denominado "muestra de registros enviados por correo" adjunto al Acta de Fiscalización N° 01-2019 de fecha 7 de enero de 2019, sírvase presentar el consentimiento de los titulares de los datos personales para realizar la transferencia de sus datos de contacto (Celular 1, Celular 2, Celular 3; Teléfono fijo 1, Teléfono fijo 2, Teléfono fijo 3; y dirección) a CMAC Piura.

5. Mediante escrito ingresado con Hoja de Trámite N°32364-2019MSC el 8 de mayo de 2019[7], la administrada absuelve requerimiento de información de la DFI, indicando lo siguiente:

5.1. Que, de la muestra de los veintidós (22) titulares del archivo Excel remitido a CMAC Piura, Sentinel cuenta con el consentimiento de dos (2) personas. Los consentimientos fueron obtenidos a través del registro voluntario de dichas personas en el registro denominado “Mi Sentinel”, con fecha 22 de setiembre de 2016 y 20 de abril de 2017.
5.2. Que, respecto a las otras veinte (20) personas, declaró que se obtuvo los datos personales de fuentes accesibles al público, los mismos que fueron recopilados durante la etapa operativa y pre-operativa de Sentinel, con información que data desde el 2001, no siendo posible especificar las fuentes específicas de origen. Sostuvo que se encuentran dentro de la limitación del consentimiento dispuesta en el numeral 2 del artículo 14 de la LPDP.

6. Mediante Oficio N° 387-2019-JUS/DGTAIPD-DFI de 10 de mayo de 2019[8], la DFI remite a la administrada el Proveído de 08 de mayo de 2019[9], en el cual se resuelve trasuntar copias fedateadas de los folios 96 a 100 del Expediente N° 132-2018-DFI al Expediente 01-2019-DFI.

7. Mediante Oficio N° 396-2019-JUS/DGTAIPD-DFI notificado el 14 de mayo de 2019[10], la DFI remite a la administrada el Proveído de 9 de mayo de 2019, mediante el cual se amplía el plazo de la fiscalización por cuarenta y cinco (45) días hábiles adicionales, los cuales se contarán a partir del 15 de mayo de 2019.

8. Con fecha 4 de junio de 2019, el Analista de Fiscalización en Seguridad de la Información de la DFI, emitió el Informe Técnico N° 88-2019-DFI-ORQR[11], referente al tratamiento de datos personales respecto a la fiscalización realizada a la administrada, concluyendo lo siguiente:

8.1. Se verificó que la administrada, a través de su sistema Sentinel (APP y web) recopila los siguientes datos: DNI, N° de celular, correo electrónico, teléfono fijo y otros[12]

[6] Folios 71 a 73
[7] Folios 79 a 81
[8] Folio 84
[9] Folio 82
[10] Folio 92
[11] Folios 93 a 94
[12] Folios 42 a 46

8.2. Se comprobó que la bandeja de salida de la cuenta de correo de la gerente de analitycs de la administrada, registra el envío de un correo electrónico a la cuenta de correo jtorres@cajapiura.pe de fecha 6 de agosto de 2018 a horas 17:37 PM, donde se describe mediante un cuadro con el título "Resumen de datos de ubicabilidad" el registro de datos personales de datos personales (celular, teléfono fijo, dirección, celular y teléfono fijo, celular y dirección, teléfono fijo y dirección, celular, teléfono fijo y dirección) con un total de 722 998 registros.

8.3. De la revisión de la muestra de los registros contenidos en el archivo Excel enviado por la administrada a CMAC Piura con fecha 6 de agosto de 2018, se verificó que estos contenían en algunos casos hasta tres (3) registros de celulares distintos y dos (2) números de teléfono fijo vinculados a una sola persona.

9. Mediante Oficio N° 624-2019-JUS/DGTAIPD-DFI notificado el 8 de agosto de 2019[13], la DFI remite a la administrada el Proveído de 15 de julio de 2019[14], en el cual se resuelve trasuntar copias fedateadas de los folios 72 a 92 del Expediente N° 132-2018-DFI al Expediente 01-2019-DFI.

10. Por medio del Informe de Fiscalización N° 110-2019-JUS/DGTAIPD-DFI-AARM del 17 de julio de 2019[15] (en adelante, el "Informe de Fiscalización"), el Analista Legal de la DFI, por los argumentos que desarrolla y la documentación que obra en el expediente, concluye que se han determinado con carácter preliminar las circunstancias que justifican la instauración de un procedimiento administrativo sancionador. Se remitió a la DFI el resultado de la fiscalización realizada a la administrada, adjuntando documentos que conforman el expediente administrativo.

11. Mediante escrito ingresado con Hoja de Trámite N° 62468-2019MSC el 3 de setiembre de 2019[16], la administrada señaló lo siguiente:

11.1. Que, ha cesado el tratamiento observado en el Informe de Fiscalización.

11.2. Que, ha dado instrucciones a Comercial y Operaciones para cesar transferencias a terceros de datos consistentes en números celulares, números de telefonía fija o direcciones, siempre que no se cuente con el consentimiento. Adjuntó comunicaciones internas.

12. Por medio de la Resolución Directoral N° 171-2019-JUS/DGTAIPD-DFI del 25 de setiembre de 2019[17] (en adelante, la "RD de Inicio"), la DFI resolvió iniciar procedimiento administrativo sancionador a la administrada, por la presunta comisión del siguiente hecho infractor:

- La administrada habría recopilado y transferido a CMAC Piura S.A.C datos personales de contacto (números de celular, números de teléfono fijo y dirección) sin contar con el consentimiento de sus titulares. Obligación establecida en el artículo 13, numeral 13.5 de la LPDP y el artículo 12 del Reglamento de la LPDP.

[13] Folio 138
[14] Folio 95
[15] Folios 119 a 122
[16] Folios 125 a 130
[17] Folios 131 a 136

13. Mediante el Oficio N°808-2019-JUS/DGTAIPD-DFI[18], se notificó la RD de Inicio a la administrada el día 11 de octubre de 2019.

14. Mediante escrito ingresado con Hoja de Trámite N°76835-2019MSC el 30 de octubre de 2019[19], la administrada presentó sus descargos alegando, principalmente, lo siguiente:

14.1. El origen de ciertas bases de datos que administra Sentinel, tanto sobre la fuente original, que ha sido fuente pública, como sobre sus fechas, han sido anteriores a la vigencia de la LPDP.
14.2. Sentinel ha requerido de un proceso de adecuación a la regulación de protección de datos bajo criterios que no siempre son claros en la ley y que, respecto a la regulación de la información obtenida de fuente pública, han ido variando ya que la interpretación que hoy sostiene la Autoridad no deriva del texto claro de la norma.
14.3. El texto legal que establece la exoneración de consentimiento para datos obtenidos de fuente pública no hace las precisiones o ampliaciones que ha hecho la autoridad administrativa en el literal i) de la RD de Inicio.
14.4. No resulta razonable exigir con rigurosidad que un administrado observe una conducta o interpretación que no está en la norma e incluso imputar infracción por tratamientos realizados antes que dicha interpretación restrictiva haya sido establecida como obligatoria o siquiera conocida por el administrado.
14.5. Los requisitos de "finalidad" que ahora establece la Autoridad para la exoneración de “consentimiento” no están en el texto de norma alguna, lo cual es determinante para evaluar si pueden ser parte de la imputación de una infracción, que ya está previamente tipificada con un texto que no incluye ningún requisito referido a "finalidad".
14.6. Antes de conocer el criterio interpretativo de la Autoridad, era perfectamente normal y razonable que los administrados considerasen que los datos de fuente pública estaban exonerados de consentimiento y que la exoneración no tenía restricciones ni los añadidos sobre finalidad que la Autoridad ha hecho al texto de la norma por vía interpretativa.
14.7. Se estaría modificando una norma que tipifica una infracción, por vía indirecta de modo contrario al principio de legalidad; asimismo, se estaría aplicando un criterio interpretativo con una suerte de "retroactividad" algo que ni siquiera se puede hacer con las normas legales.
14.8. Sentinel se ha conducido acatando una norma de acuerdo a su texto y está dispuesta a acatar la nueva interpretación que la Autoridad ha introducido en la norma, esperando que se comprendan tres cosas: i) en la etapa pre operativa y de inicio de operaciones el marco legal no existía, ii) se han conducido en el entendido de que el marco legal les daba la cobertura de una exoneración, iii) noticiados del criterio de la Autoridad, se ha dispuesto la adecuación, que es un proceso no exento de dificultades.
14.9. Siguiendo el razonamiento de la Autoridad, en el sentido que los datos obtenidos de fuente pública (números telefónicos) sólo podrían considerarse exonerados si son tratados para la finalidad que tenían al ser puestos a disposición en la fuente pública, corresponde preguntar ¿cuál podría ser la finalidad de un banco de datos, puesto a disposición del público que contenga números telefónicos, que no sea el contacto telefónico? Aún con la restricción

[18] Folio 138
[19] Folios 139 a 200

de finalidad incorporada por la Autoridad, los tratamientos fiscalizados, en este caso concreto pueden considerarse exonerados del consentimiento.

14.10. Adjunta en Anexos 1-A y 1-B el screen de la plataforma con las explicaciones de cómo acceder, informarse, dar o no su consentimiento, así como el documento informativo de términos y condiciones, que, según alega, acreditan que la plataforma "Mi Sentinel" es un medio idóneo de otorgamiento de consentimiento.

14.11. Las conductas de colaboración probadas y glosadas en la RD de Inicio; de respeto a los criterios de la Autoridad, así como de enmienda de los actos fiscalizados no han sido reconocidos, sin explicación alguna. La RD de Inicio, en su literal m) menciona que las conductas de remedio o enmienda, "no alcanza como enmienda" sin explicar ni motivar por qué las descarta.

14.12. De acuerdo a lo señalado en el artículo 126° del Reglamento de la LPDP, solicita que de corresponder imponer una multa, el monto se determine apreciando los atenuantes que permiten establecerlo por debajo del rango previsto, considerando que: i) la administrada ha colaborado siempre con la Autoridad, ii) al tomar conocimiento del criterio distinto sobre la exoneración por fuente pública, se ha reconocido que el tratamiento debía cesar, iii) se ha acreditado en el expediente las acciones de enmienda, y iv) se ha explicado las circunstancias de tiempo y origen de las fuentes públicas, que a su vez explican la oportunidad en que ha acontecido la enmienda.

15. Por medio de la Resolución Directoral N° 236-2019-JUS/DGTAIPD-DFI del 29 de noviembre de 2019[20], la DFI dio por concluidas las actuaciones instructivas correspondientes al procedimiento sancionador.

16. Mediante Informe Final de Instrucción N° 153-2019-JUS/DGTAIPD-DFI del 29 de noviembre de 2019[21] (en adelante, el "IFI"), la DFI remitió a la Dirección de Protección de Datos Personales (en adelante, la "DPDP") los actuados para que resuelva en primera instancia el procedimiento administrativo sancionador iniciado, recomendando lo siguiente:

- Imponer sanción administrativa de multa ascendente a veinte unidades impositivas tributarias (20 UIT) a la administrada por el cargo acotado en el Hecho Imputado N° 1, por 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 Nº 29733 y su Reglamento."*

17. El IFI así como la Resolución Directoral N°236-2019-JUS/DGTAIPD-DFI fueron notificados a la administrada mediante Oficio N°999-2019-JUS/DGTAIPD-DFI de fecha 6 de diciembre de 2019[22].

18. A través del escrito ingresado con Hoja de Trámite N°89193-2019MSC el 18 de diciembre de 2019[23], la administrada presentó sus descargos al IFI, precisando lo

[20] Folios 204 a 205
[21] Folios 206 a 215
[22] Folio 216
[23] Folios 217 a 247

siguiente sobre la existencia de los atenuantes que el Artículo 126 del Reglamento de la LPDP tiene previstos:

18.1. La colaboración con las acciones de la autoridad, es un atenuante que merece evaluarse y que no ha sido tratada ni mencionada por la Autoridad.

18.2. En cuanto al reconocimiento de las infracciones merece ser evaluado considerando que la excepción de consentimiento por razón de "fuente pública" no contiene en su texto expreso las adiciones y precisiones sobre las finalidades que luego ha desarrollado la Autoridad en consultas, las mismas que, al no tener carácter vinculante, no resultan exigibles en los mismos términos en los que son las normas vigentes. Una vez establecido el criterio interpretativo de la Autoridad (cuya exigibilidad no era razonable antes), en este proceso, Sentinel reconoce la infracción.

18.3. Las acciones de enmienda se han realizado y la Autoridad ha reconocido que se han tomado las medidas internas para cesar el tratamiento considerado inadecuado y sin embargo se ha afirma que "no alcanzan", sin mayor explicación. Una conducta de enmienda, consiste en "dejar de hacer aquello que se hacía inadecuadamente" y eso es lo que ha acontecido en este caso.

18.4. La DFI parece entender que la enmienda consistiría en "obtener el consentimiento" que no se obtuvo antes, lo cual no parece un enfoque razonable: primero: porque el tratamiento ya está realizado y un consentimiento posterior es contrario al requisito de que sea "previo", razón por la que ni subsana ni enmienda; segundo: porque asumir que es posible que "la enmienda consiste en un obtener un consentimiento posterior que lo subsane" supondría la "desaparición de la infracción" y no un "atenuante" que es como está regulado en la norma; y tercero porque si el criterio fuese el de subsanar el consentimiento sobre un tratamiento que ya se realizó (además de ser jurídicamente inútil, por no ser previo) sería físicamente imposible, porque no es posible retroceder el tiempo para obtener un consentimiento (que debe ser previo) sobre algo que ya se hizo en el pasado.

18.5. Sobre las consideraciones expuestas en el literal “d” del numeral 6 del IFI se desprende una generalización del criterio de acuerdo al cual los datos de contacto como domicilio o teléfono no serían información con relevancia crediticia, y por tanto información que las Cepirs no pueden tratar. Dicha generalización resulta contraria a la realidad del mercado crediticio tal como ha sido reconocido por el INDECOPI:

18.5.1. La Resolución N° 747-2000 de la Comisión de Protección al Consumidor, que reconoce que el proveedor de información crediticia puede incorporar información adicional a la expresamente autorizada, siempre que sea objetiva (y los datos de contacto lo son).

18.5.2. El Tribunal de Defensa de la Competencia, en la Resolución N° 0571-2001 deja establecido que el dato referido al domicilio de una persona es relevante para la evaluación del riesgo

18.6. Dentro de la información de riesgo definida en la Ley 27489 incorpora toda la información relevante para una adecuada evaluación de la solvencia económica vinculada principalmente a su capacidad y trayectoria de endeudamiento y pago (evaluación de riesgo crediticio), dentro de la cual resulta útil y pertinente la información de contacto obtenida y tratada para estas finalidades.

19. Mediante Resolución Directoral N.º 1464-2020-JUS/DGTAIPD-DPDP del 18 de setiembre de 2020; la DPDP resolvió sancionar a SENTINEL PERÚ S.A. con la multa ascendente a veinte unidades impositivas tributarias (20UIT) por la comisión de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP.

20. El 13 de octubre de 2020, Sentinel presentó recurso de apelación contra la Resolución Directoral N° 1464-2020-JUS/DGTAIPD-DPDP del 18 de setiembre de 2020.

21. Mediante Resolución Directoral 12-2021-JUS/DGTAIPD, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales declaró fundado el recurso de apelación y, en consecuencia "NULA la Resolución Directoral N° 1464-2020-JUS/DGTAIPD-DPDP del 18 de setiembre de 2020, correspondiendo RETROTRAER el procedimiento administrativo sancionador hasta el momento previo a la emisión de la resolución de sanción."

II. Competencia

22. 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.

23. En tal sentido, la autoridad que debe conocer el presente procedimiento administrativo 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

24. 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 del Procedimiento Administrativo General (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[24].

25. 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[25].

[24] **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."

[25] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 003-2013-JUS**
"**Artículo 126.- Atenuantes.**

26. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 257 de la LPAG[26], 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.

IV. Cuestiones en discusión

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

27.1. Si la administrada es responsable por el siguiente hecho infractor:

- La administrada habría recopilado y transferido a CMAC Piura S.A.C datos personales de contacto (números de celular, números de teléfono fijo y dirección) sin contar con el consentimiento de sus titulares. Obligación establecida en el artículo 13, numeral 13.5 de la LPDP y el artículo 12 del Reglamento de la LPDP, con lo cual se configuraría 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 Nº 29733 y su Reglamento."*

27.2. 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.

27.3. Determinar de ser el 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

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

"Artículo 5. Principio de consentimiento

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"

[26] **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."

29. 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 cual 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."*

30. 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[27] del Reglamento de la LPDP, siendo tales requisitos de ser otorgado de forma previa, libre, expresa e inequívoca, y

[27] 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 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."

de manera informada. La omisión de alguno de estos requisitos implica la nulidad de su obtención.

31. 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[28], no encontrándose inmerso en ninguna de ellas la administrada que le permita legitimar el tratamiento realizado de los datos personales de aquellos titulares cuya información de contacto (números de celular, números de teléfono fijo y dirección) fue finalmente transferida a CMAC Piura, según se aborda más adelante.

32. De los hechos expuestos y analizados, este Despacho observa que la administrada, efectivamente, ha realizado tratamiento indebido de datos personales (números telefónicos celulares y/o móviles y fijos, así como direcciones) sin consentimiento de sus titulares. Puesto que se tomó una muestra de 22 casos del total de setecientos veintidós mil novecientos noventa y ocho (722,998) registros que se remiten a CMAC Piura, de los cuales en veinte de ellos no se cuenta con el consentimiento, puesto que la administrada señaló que fueron obtenidos a través de fuentes de acceso al público, indicando además que fueron recopilados en una etapa pre operativa y operativa de la empresa, información que data del año 2001, señalando que no puede identificar las fuentes específicas. Por lo que, sostiene que se encuentran dentro de la limitación del consentimiento dispuesta en el numeral 2 del artículo 14° de la LPDP.

[28] **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.
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**"**.

33. A efectos de desarrollar el pronunciamiento de este Despacho, resulta importante evaluar las implicancias del tratamiento de datos personales conformado por aquella información y/o datos referidos a la solvencia patrimonial y de crédito, que se encuentran comprendidas en la Ley N° 27489, "Ley que regula las Centrales Privadas de Información de Riesgos y de protección al titular de la información - CEPIRS" (en adelante, la "Ley de CEPIRS") que le es aplicable a la administrada en su calidad de central privada de información de riesgos, en concordancia, claro está, con la observancia obligatoria de la normativa de protección de datos personales nacional.

34. En tal sentido, para el caso particular de las CEPIRS es necesario enfocar el análisis a partir de lo que establece el principio rector de finalidad desarrollado por la LPDP para determinar si la administrada actuó de manera legitimada o no. El artículo 6 de la LPDP[29], sobre el principio de finalidad establece que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita, no debiendo extenderse el tratamiento de los mismos a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación. Así también el artículo 8 del Reglamento de la LPDP complementa la definición de este principio 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. (…)*[30]

35. Sobre este principio rector, la Autoridad Nacional de Protección de Datos Personales precisó a través de Oficio N°262-2013-JUS/DGPDP de 22 de agosto de 2013 lo siguiente:

"En cuanto al tratamiento de los datos personales, es importante mencionar que la protección de los datos personales se rige por determinados principios rectores contemplados en la Ley, entre los que destaca el principio de finalidad, que dispone que los datos personales se tratan atendiendo a las limitaciones que marca la finalidad determinada, explícita, lícita y autorizada, ya sea por el titular de los datos (el ciudadano de cuyos datos se trata) o por la norma legal que regula la función de la entidad administrativa que tiene a su cargo el banco de datos personales.

Lo expuesto en el párrafo anterior quiere decir que aquello que se puede hacer con los datos es aquello que responda a la finalidad "autorizada" y no se extiende a otra u otras finalidades que no hayan sido establecidas de manera inequívoca como tal al momento de su recopilación." (Subrayado propio)

36. Consecuentemente, para el caso de las CEPIRS la finalidad de tratamiento proviene de la autorización expresa y específica que la Ley de CEPIRS les otorga para tratar

[29] **Ley N° 29733, Ley de Protección de Datos Personales**
"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."

[30] **Reglamento de la LPDP:**
"Artículo 8.- Principio de finalidad.
En atención al principio de finalidad se considera 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.
Tratándose de banco de datos personales que contengan datos sensibles, su creación solo puede justificarse si su finalidad además de ser legítima, es concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales.
Los profesionales que realicen el tratamiento de algún dato personal, además de estar limitados por la finalidad de sus servicios, se encuentran obligados a guardar secreto profesional."

datos personales de información de riesgo sin consentimiento de sus titulares, conforme se desarrolla a continuación.

37. El objeto de la Ley de CEPIRS es regular el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares y promoviendo la veracidad, confidencialidad y uso apropiado de dicha información. [31] En tal sentido, dicha ley define a las CEPIRS[32] como aquellas empresas que recopilan y tratan[33] información de riesgos relacionada con personas naturales o jurídicas con el único propósito de difundir reportes de crédito sobre éstas que permita al solicitante y/o interesado evaluar la solvencia económica vinculada principalmente a la capacidad y trayectoria de endeudamiento y pago de una persona natural o jurídica identificada por dicho solicitante.

38. Ahora bien, es pertinente acotar que el término "difundir" debe entenderse -en observancia de la normativa de protección de datos personales y respeto de los derechos de los titulares que recoge como guía en su regulación la Ley de CEPIRS- como la actividad de entregar o transmitir reportes de crédito que contengan información de riesgos, sea propia o de terceros, a aquellas personas que lo soliciten.

39. El inciso 7.1 de la Ley de CEPIRS establece que *"Las CEPIRS podrán recolectar información de riesgos para sus bancos de datos tanto de fuentes públicas como de fuentes privadas, sin necesidad de contar con la autorización del titular de la información, entendiéndose que la base de datos se conformará con toda la información de riesgo."* (Subrayado propio). Asimismo en el literal b) del artículo 9 de la Ley de CEPIRS establece como uno de los lineamientos generales para la recopilación y tratamiento de información de riesgos a cargo de las CEPIRS que *"la información recolectada sólo podrá ser utilizada para los fines señalados en la presente Ley"*

40. Conforme se describe en el literal b) del artículo 2 de la Ley de CEPIRS, la información de riesgos destinada a estar comprendida en los reportes de crédito que se encuentran facultados a emitir las CEPIRS en virtud de la mencionada ley se encuentra conformada por toda aquella *"información relacionada a obligaciones o antecedentes financieros, comerciales, tributarios, laborales, de seguros de una persona natural o jurídica que permita evaluar su solvencia económica vinculada principalmente a su capacidad y trayectoria de endeudamiento y pago"*. Por su lado, los reportes de crédito y/o crediticios se definen en el literal e) del artículo 2 de la Ley de CEPIRS como *"toda*

[31] **Artículo 1 de la Ley de CEPIRS:**
"Artículo 1.- Objeto de la ley
La presente Ley tiene por objeto regular el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, confidencialidad y uso apropiado de dicha información."

[32] **Artículo 2, literal a) de la Ley de CEPIRS:**
"Artículo 2.- Definiciones
Para los efectos de esta Ley, se entiende por:
a) Centrales privadas de información de riesgos (CEPIRS).- Las empresas que en locales abiertos al público y en forma habitual recolecten y traten información de riesgos relacionada con personas naturales o jurídicas, con el propósito de difundir por cualquier medio mecánico o electrónico, de manera gratuita u onerosa, reportes de crédito acerca de éstas. No se consideran CEPIRS, para efectos de la presente Ley, a las entidades de la administración pública que tengan a su cargo registros o bancos de datos que almacenen información con el propósito de darle publicidad con carácter general, sin importar la forma como se haga pública dicha información."

[33] El literal i) del artículo 2 de la Ley de CEPIRS define al tratamiento de información de riesgos y/o crediticia como "Toda operación o conjunto de operaciones o procedimiento técnico, de carácter automatizado o no, que permitan a las CEPIRS acopiar, almacenar, actualizar, grabar, organizar, sistematizar, elaborar, seleccionar, confrontar, interconectar, disociar, cancelar y, en general, utilizar información de riesgos para ser difundida en un reporte de crédito." (Subrayado propio)

comunicación escrita o contenida en algún medio proporcionada por una CEPIR con información de riesgos referida a una persona natural o jurídica, identificada."

41. Analizado el cuerpo normativo de la Ley de CEPIRS, se desprende que dicha ley únicamente habilita a las centrales de riesgo a realizar el tratamiento de datos de naturaleza crediticia (información de riesgos), sin consentimiento de sus titulares, con la finalidad de emitir reportes de créditos que permitan conocer cómo se comportan los sujetos de crédito en el tiempo, a efectos de que todo interesado o solicitante de este tipo de reportes respecto de una persona natural o jurídica en particular, finalmente, decida si establece o no vínculo crediticio y/o contractual alguno con ella.

42. Esta legitimación de tratamiento de datos referidos a información de riesgos contenidos en los reportes de crédito, en tanto no es necesario el consentimiento de sus titulares ha sido reconocido por el Tribunal Constitucional, toda vez que ello permite generar confianza en el sistema financiero, pero solo en tanto esté restringido a información de riesgos o de tipo crediticio como menciona el Tribunal Constitucional en el considerando 6 de la Sentencia recaída en el Expediente Nº 03700-2010-PHD/TC:

"6. Sin embargo, es necesario precisar que resulta legítimo y acorde con el derecho a la libertad de contratación, que exista un flujo continuo de información de riegos crediticios en el mercado, pues solo así se puede generar confianza en el sistema financiero para el otorgamiento de créditos y su consiguiente recuperación, en la medida que el tratamiento de este tipo de datos permite, tanto a personas jurídicas como a personas naturales, conocer el comportamiento en el tiempo de los sujetos de crédito en general (historial crediticio: endeudamiento, capacidad de pago, voluntad de pago), para así tomar decisiones adecuadas en tomo al ofrecimiento de créditos, lo cual repercute directamente en la economía nacional (requisitos para el acceso al crédito, tasas de interés, por ejemplo). Por tal razón, y dado que la difusión de este tipo de datos en específico cumple un fin constitucionalmente legítimo, no es necesario que para su tratamiento se recabe el consentimiento de su titular, dado que se entiende que la permisibilidad legal resulta legítima solo y exclusivamente para información de tipo crediticio." (Subrayado propio).

43. Las centrales de información de riesgos no se encuentran legalmente facultadas a tratar para efectos de la generación de los reportes de créditos datos personales distintos a aquella información de riesgo -tal cual ha sido ésta definida y conceptualmente delimitada por la Ley de CEPIRS -, sin consentimiento de sus titulares. Consecuentemente, las CEPIRS no se encuentran legitimadas bajo el amparo de la ley especial que las regula incluir en estos reportes que genere a sus clientes o usuarios datos personales como números telefónicos, direcciones y/o cualquier otro dato que no se encuentre comprendido en la categoría de información de riesgos, al no tener naturaleza crediticia que permita dar a conocer el comportamiento y/o desenvolvimiento económico en el sistema financiero de su titular, mucho menos a comercializar estos datos personales ajenos a información de riesgos sin consentimiento previo y debidamente informado de sus titulares justificando el tratamiento de los mismos bajo el amparo de la Ley de CEPIRS. Este razonamiento también ha sido acogido en el considerando 19 de la Sentencia recaída en el Expediente Nº 03700-2010-PHD/TC:

"19. Teniendo en cuenta el contenido de la citada normatividad, este Tribunal advierte que la ley ha habilitado a las Cepirs para que efectúen el tratamiento de datos de naturaleza crediticia, esto con la finalidad de difundir el historial o comportamiento crediticio de personas naturales como jurídicas el sistema financiero, promoviendo así su fortalecimiento.

En tal sentido, se entiende que la habilitación legal del tratamiento de datos a partir de la Ley 27489, se encuentra limitada solo a datos crediticios y no otros." (Subrayado propio).

44. Sustentar lo contrario, o inclusive intentar extender la definición de información de riesgos a datos que no poseen naturaleza crediticia, únicamente fomentaría un uso indiscriminado y arbitrario de datos personales sin consentimiento de sus titulares, atentando no solo contra el propósito de creación y puesta a disposición de este tipo de banco de datos administrados por las CEPIRS que lo que persigue como fin último es la generación de confianza en el sistema financiero, sino también contra el derecho a la autoderminación informativa.

45. A criterio de este Despacho el tratamiento de los datos personales de contacto, constituidos estos, en el presente caso, por los domicilios y números telefónicos efectuados con fines comerciales por la administrada, sin consentimiento válido de sus titulares no se encuentra legitimado por la Ley de CEPIRS. En tal sentido, cualquier tipo tratamiento relacionado a dichos datos de contacto, así como a cualquier otro que no tenga naturaleza crediticia o escape a la definición clara y expresa que se desprende de la Ley de CEPIRS al aludir al concepto de información de riesgos, resulta ajeno a la finalidad de tratamiento autorizado expresamente en dicha ley, constituyendo una intromisión a la privacidad de sus titulares y una violación del derecho fundamental a la autodeterminación informativa.

46. En este sentido, este Despacho no puede estimar lo argumentado por la administrada al señalar que realizó el tratamiento de los datos personales de contacto amparándose en la Ley de CEPIRS, toda vez que los números telefónicos y direcciones domiciliarias no constituyen información de riesgo y/o crediticia que pueda ser tratada sin consentimiento de sus titulares en los términos de esta ley especial. Para una finalidad distinta de tratamiento a aquella permitida y avalada por la Ley de CEPIRS la administrada debió contar con el consentimiento válido, en los términos de la LPDP y su Reglamento, de cada uno de los titulares de los datos personales de contacto, contenidos en el la información enviada vía correo electrónico por la administrada a CMAC Piura, con fecha 6 de agosto de 2018, conforme a la muestra de los 20 registros mencionados, lo cual no ha sido acreditado en el presente procedimiento por Sentinel.

47. En línea con lo aquí expresado, tampoco cabe amparar lo argumentado por la administrada en el extremo de que la exclusión de los datos de contacto (números telefónicos y domicilios tratados sin consentimiento por Sentinel para fines comerciales) resulte contrario a la realidad del mercado crediticio, en tanto dichos datos no se encuentran directamente relacionados con obligaciones o antecedentes financieros, comerciales, tributarios, laborales o de seguros de una persona en particular que resulten relevantes para permitir evaluar su solvencia económica vinculada a su capacidad y trayectoria de endeudamiento y pago.

48. Sin embargo, la administrada ha centrado su defensa en señalar que los datos de contacto que forman parte de la información remitida a CMAC Piura fueron obtenidos de diversas fuentes accesibles al público, sin identificar cuáles fueron éstas, con anterioridad a la entrada en vigencia de la LPDP (información que data del año 2001), acotando principalmente que i) dicho tratamiento se encuentra excluido de la obligación de contar con consentimiento de sus titulares conforme el numeral 2 del artículo 14 de la LPDP y ii) que el texto legal que establece la exoneración de consentimiento para datos obtenidos de fuente pública no hace las precisiones o ampliaciones que ha desarrollado la autoridad administrativa en la RD de Inicio (particularmente, respecto al fundamento contenido su literal “i”- Folios 133 reverso y 134)

49. Al respecto, resulta importante señalar que por el solo hecho que un dato personal se encuentre contenido en cualquier tipo de fuente accesible al público, ello no implica que este dato personal pueda ser tratado de manera amplia para fines comerciales como advierte este Despacho ha acontecido en el presente caso. Si bien el artículo 14 de la LPDP establece que no se requiere el consentimiento de los titulares de los datos personales para efectos de su tratamiento cuando se trate de datos contenidos o destinados a ser contenidos en fuentes accesibles al público, ello únicamente se encuentra limitado -en concordancia con el espíritu proteccionista de la normativa de protección de datos personales nacional reflejado en los principios rectores a través de los cuales actúa-, al tratamiento de acceso y/o consulta, pudiendo permitir a criterio de este Despacho un tratamiento de recopilación pero, únicamente, con fines de llevar a cabo dicho acceso o consulta posterior de manera directa en atención de los fines para los cuales fueron creadas estas fuentes. Esta excepción a la regla de obtención del consentimiento, se encuentra supeditada a la observancia de los principios generales de los cuales parte la regulación de protección de datos personales, siendo ello reconocido en el último párrafo del artículo 17 del Reglamento de la LPDP: *"(…) El tratamiento de los datos personales obtenidos a través de fuentes de acceso público deberá respetar los principios establecidos en la Ley y en el presente reglamento."* (Subrayado propio)

50. No se trata pues de un criterio impuesto con posterioridad a la vigencia de la LPDP y su Reglamento o, menos aún, de una interpretación antojadiza de la Autoridad Nacional de Protección de Datos Personales que busque imponer restricciones inexistentes como alega impetuosamente la administrada en sus descargos. Por el contrario, nos encontramos ante un nivel proteccionista de datos personales reconocido a nivel constitucional que data, inclusive, desde antes de la expedición de la Ley de CEPIRS y de la LDPD y su Reglamento con el reconocimiento de los derechos a la intimidad, al honor y a la propia imagen (inciso 7 del artículo 2 de la Constitución Política del Perú de 1993- en adelante, la "Constitución"), así como el derecho de autodeterminación informativa desarrollado en el inciso 6 del artículo 2 de la Constitución al establecer que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

51. Es en reconocimiento de tales derechos constitucionales que cualquier tipo de normativa expedida, especialmente, la Ley de CEPIRS, que como ha sido expuesto delimita las competencias de las centrales de información de riesgos para efectuar tratamiento de datos únicamente de naturaleza crediticia, exceptuando de la regla de obtención de consentimiento de su titular para dicho tratamiento en aras de permitir conocer el comportamiento económico y financiero en el tiempo de un sujeto de crédito; si bien responde a un fin legítimo que es fortalecer el desarrollo financiero y económico en general debe ser interpretada en consonancia y respeto al derecho a la protección de datos personales. Es en este sentido que la propia Ley de CEPIRS recoge en su objeto dicho reconocimiento al establecer que regulará el suministro de información de riesgos, "*garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, confidencialidad y uso apropiado de dicha información."* (Artículo 1 de la Ley de CEPIRS)

52. Por su lado, la LPDP y su Reglamento desde sus inicios contempla como principios rectores a los de finalidad y consentimiento que son el punto de partida que debe regir toda modalidad de tratamiento de datos personales para una debida protección acorde con su reconocimiento constitucional. En tal sentido, la LPDP, en su artículo 12, reconoce a estos principios como piedra angular en materia de protección de datos personales:

"Artículo 12. Valor de los principios

La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.
Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia". (Subrayado propio)

53. En este orden de ideas, este Despacho suscribe lo expuesto por la DFI en el literal "i" de la RD de Inicio (Folios 133 reverso y 134) respecto a 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. Aunque la administrada no haya identificado cuáles son las fuentes de acceso público de las cuales recopilaron los números telefónicos y direcciones domiciliarias, para efectos de explicación, resulta oportuno señalar, a manera de ejemplo, que para el caso de los directorios o guías telefónicas que contengan información de abonados, el tratamiento de consulta y/o acceso a la información contenida en este tipo de fuente debe entenderse limitado para uso personal y/o doméstico o en el marco de una relación contractual vigente con el titular del número telefónico, en el supuesto de necesidad de contactar previo conocimiento de la persona por parte del interlocutor. En un supuesto distinto y para finalidades que exceden a la de una necesidad de contacto para fines personales o relacionados a un vínculo contractual previo debe regir la regla de obtención de consentimiento previo del titular del número telefónico para fines, por ejemplo, comerciales o publicitarios. Ahora bien, para fines publicitarios o comerciales, 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. En tal sentido, se podría utilizar los datos obtenidos de fuentes accesibles al público para, además de la finalidad para la que ha sido creada, contactar al titular del dato personal para obtener su consentimiento para diversas finalidades.

54. En el presente caso, se observa que la administrada no ha presentado prueba fehaciente de contar con el consentimiento previo de los titulares de los números telefónicos que obran en su banco de datos para fines comerciales, dentro de los cuales se encuentra la muestra de veinte registros transferidos a CMAC Piura con fecha 6 de agosto de 2018, y que según alega la administrada habrían sido recopilados de diversas fuentes de acceso al público (aunque no habría identificado cuáles ni tampoco acreditó que los datos de contacto hayan sido obtenidos de fuentes de acceso al público).

55. Siguiendo con los ejemplos de finalidades de uso de fuentes accesibles al público, conforme al nivel de protección de un uso adecuado de los datos personales que se desprende de la LPDP, desde una visión integral de su cuerpo normativo, para el caso de las búsquedas en RENIEC, para verificar la identidad de personas y evitar

suplantaciones, ello en el marco de, por ejemplo, encontrarse dentro de un contexto precontractual con la persona de la cual se busca información. En el supuesto hipotético de que la administrada hubiese recopilado las direcciones de RENIEC, el tratamiento dado a los mismos no se encontraba autorizado *per se* para fines comerciales, con lo cual debió contar con el consentimiento de sus titulares, lo cual tampoco ha sido acreditado en el presente procedimiento.

56. Tal es la relevancia de los principios de consentimiento y finalidad establecidos en la LPDP, que en la definición de fuentes accesibles para el público[34] se establece que este tipo de banco de datos personales pueden ser consultados por cualquier persona, delimitando con ello a una modalidad de acceso para consulta; la cual se encuentra delimitada por los principios rectores de la LPDP para un tratamiento razonable y acorde con la finalidad de creación de la fuente de acceso al público de la cual se obtienen los datos personales.

57. En el presente caso, conforme ha sido señalado por la DFI en su Informe Final de Instrucción, se ha verificado que la administrada realizó la recopilación y transferencia de los datos personales extraídos de las fuentes de acceso al público, sin haber contado con la obtención del consentimiento válido por parte de sus titulares para la comercialización de los mismos por parte de Sentinel.

58. 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, ello debe ser enmarcado dentro del ámbito de la ley, en observancia del principio rector del consentimiento, lo cual no ha cumplido en el presente caso.

59. Conforme lo hasta aquí desarrollado, en ningún caso la información que fuera recopilada de fuentes de acceso al público como las aquí mencionadas, a manera de ejemplo, facultan al usuario de las mismas a incorporarlas en bancos de datos para un tratamiento y finalidad que no hubieran sido consentidos válidamente conforme lo establecido en la normativa de protección de datos personales.

60. 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 y Protección de Datos Personales ("DGTAIPDP") a través del Oficio N° 749-2018-JUS/DGTAIPD del 7 de agosto de 2018 en la emisión de una opinión consultiva: *"(…) 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,*

[34] Artículo 2, numeral 11 de la LPDP:
"**Artículo 2. Definiciones.**
Para todos los efectos de la presente Ley, se entiende por:
(...)
11. Fuentes accesibles para el público. Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento"

deberá solicitarse el consentimiento conforme al artículo 5 y el artículo 13, inciso 13.5 de la LPDP"

61. Así también, la DGTAIPD emitió opinión consultiva respecto al tratamiento de datos personales que formen parte de la información de riesgos, según las competencias otorgadas por la Ley de CEPIRS. Al respecto, la DGTAIPDP, a través del Oficio N° 146-2018-JUS/DGTAIPD del 14 de marzo de 2018 se pronunció conforme a seguir: *"(…) las centrales de riesgo no requieren consentimiento para el tratamiento de datos personales regulado por la Ley 27489 en el marco de las competencias asignadas, sin embargo, para transferir dichos datos personales para otras finalidades deberán contar con el consentimiento del titular del dato personal. (…)"*

62. Las referidas opiniones consultivas han sido emitidas en cumplimiento de la función orientadora que le ha sido atribuida a la Autoridad Nacional de Protección de Datos Personales en la LPDP para absolver consultas relacionadas al sentido de normas vigentes en la materia[35], es decir, aquella regulación previamente establecida en la misma, no introduciendo con ello, como alega la administrada, una modificación normativa a través de la generación e imposición de un criterio ajeno a lo establecido en la ley, contraviniendo con ello el principio de legalidad, según percepción de Sentinel.

63. En consecuencia, para este Despacho no resulta amparable el argumento de la administrada, respecto a que, era perfectamente normal y razonable que los administrados considerasen que los datos de fuente pública estaban exonerados de consentimiento y que dicha exoneración no tenía restricciones, toda vez que, como ha sido expuesto, el tratamiento de los datos personales contenidos en fuentes de acceso al público, se encontraba previamente delimitado a la observancia y actuación conforme a los principios de consentimiento y finalidad contenidos en la LPDP. No se trata de la generación de un nuevo criterio sino, por el contrario, del resultado de una revisión integral de la normativa de protección de datos personales, la misma que otorgó a los a6dministrados un período de adecuación pertinente para que adecuen el tratamiento de datos personales y la gestión de sus bancos de datos a la misma. Por lo tanto, no resulta aceptable justificar una falta de adecuación a la LPDP y su Reglamento o continuar incurriendo en su incumplimiento en función a una interpretación aislada y conveniente del numeral 2 del artículo 14 de la LPDP, omitiendo la observancia de los principios rectores de consentimiento y finalidad, principalmente.

64. 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 procederá a evaluar la idoneidad de las actuaciones realizadas por la administrada respecto al hecho infractor imputado. Para ello, de la documentación obrante en el expediente se tiene lo siguiente:

---

[35] **Inciso 10 del artículo 33 de la LPDP:**
"Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales
La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:
(…)
10. Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
(…)"

i) Comunicación del cese de tratamiento observado en el Informe de Fiscalización N° 110-2019-JUS/DGTAIPD-IFI-AARM y documentos internos de fecha 8 de agosto de 2019 dirigidos a las áreas de Comercial y Operaciones conteniendo instrucciones para el cese de transferencia a terceros de datos de contacto (números telefónicos móviles y/o celulares, números telefónicos fijos y direcciones) siempre que no se cuente con el consentimiento respectivo del titular. Dichas comunicaciones fueron presentadas por la administrada en su escrito ingresado el 3 de setiembre de 2019 con Hoja de Trámite N°62468-2019MSC (Folios 125 a 130)

ii) Screen de la plataforma "Mi Sentinel", así como el documento "Términos y Condiciones" que, según alega la administrada, reflejaría que se trata de un medio idóneo para la obtención del consentimiento de los titulares. La administrada señaló que "Mi Sentinel", ha servido para obtener consentimientos, que aun cuando no cubran el total del banco de datos, demuestran su voluntad de cumplimiento con la normativa de protección de datos personales. Dicha documentación fue presentada mediante escrito ingresado con Hoja de Trámite N°76835-2019MSC el 30 de octubre de 2019 (Folios 145 a 150)

65. Respecto a la comunicación de la administrada del cese de tratamiento observado en el Informe de Fiscalización (Folio 126), este Despacho advierte que la mera declaración en tal sentido de la administrada no crea convicción respecto a que se haya producido efectivamente el cese del tratamiento de los datos transferidos a CMAC Piura. Ello, en tanto, la administrada no ha presentado prueba fehaciente de haber eliminado aquellos datos de contacto de cuyos titulares no haya obtenido el consentimiento respectivo o que, en todo caso, para adecuar su actuar a la observancia de la LPDP haya intentado regularizar la prexistencia en su banco de datos y tratamiento que realiza sobre los mismos. Por tanto, dicha declaración de cese no puede ser valorada como una acción de enmienda total para efectos de atenuar la responsabilidad de la administrada.

66. En cuanto a los documentos internos dirigidos a las áreas de Comercial y Operaciones de la administrada, conteniendo instrucciones para el cese de transferencia a terceros de datos de contacto (Folios 127 a 130), este Despacho considera que dicha acción no alcanza como enmienda del hecho infractor constituido por la recopilación y almacenamiento en su banco de datos y posterior transferencia de los datos de contacto a CMAC Piura, en tanto configura órdenes a futuro. Asimismo, dado que ya remitió la información a terceros, es decir la información ha salido de su esfera de control, no es posible que se enmiende la situación, puesto que ya no tiene el control sobre los datos personales que ha transferido sin consentimiento.

67. Sin perjuicio de lo aquí señalado, las órdenes internas a nivel de Sentinel para el cese de transferencia a terceros de datos de contacto, a criterio de este Despacho, constituyen una manifestación de la voluntad de la administrada de adecuar su actuar a partir del 8 de agosto de 2019 (fecha de las comunicaciones internas) a la correcta observancia de la normativa de protección de datos personales a futuro, aunque como se ha desarrollado en los párrafos anteriores de este considerando se aprecia que su objetivo no es remediar el tratamiento indebido respecto a los datos correspondientes a la muestra revisada que fueron recopilados y transferidos a CMAC Piura.

68. Finalmente, respecto a que la plataforma "Mi Sentinel" es un medio idóneo de otorgamiento de consentimiento por parte de los titulares de los datos personales de

contacto, este Despacho concuerda con lo señalado en los literales p) a t) contenidos en las páginas 12 a 16 del Informe Final de Instrucción (Folios 211 reverso a 213 reverso), en tanto la fórmula empleada por la administrada para la obtención del consentimiento de los usuarios que se registren en "Mi Sentinel" para la recopilación y posteriores tratamientos de sus datos personales de contacto no cumple con ser libre y expreso en términos del artículo 12 de Reglamento de la LPDP.

69.De la revisión de oficio realizada a la plataforma "Mi Sentinel" por la DFI, conforme obra en el Informe Final de Instrucción y en los Folios 201 a 203 del expediente, se verificó que la administrada tenía implementado dos recuadros para ser marcados por el usuario de su sitio web, para efectos de su registro en la plataforma, en el cual se mostraban las siguientes opciones:

"□ Acepto los términos y condiciones de Acceso y Uso.
□ Otorgo consentimiento para la transferencia de mis datos personales, conforme la cláusula 4.2 de los presentes términos y condiciones."

70. La DFI verificó que para proceder con el registro el usuario necesariamente tiene que marcar la opción "Acepto los términos y condiciones de Acceso y Uso" (Folios 201 a 202), advirtiendo que, al marcar esta opción, el usuario estaría aceptando el contenido íntegro de dicho documento. Dicho documento contempla en su cláusula 4.2 la posibilidad de transferir los datos personales que están siendo recopilados del usuario a través de dicha plataforma (como DNI, correo electrónico y número de celular y/o móvil) a terceros con fines comerciales y publicitarios, sin otorgarles la posibilidad de manifestar su consentimiento de forma expresa respecto a que sus datos personales sean tratados por empresas distintas (Empresas Asociadas a Sentinel, Verifica Perú S.A y Empresas Asociadas a Verifica Perú S.A) a la cual están proporcionado sus datos personales al completar el formulario para registrarse como usuarios de la plataforma "Mi Sentinel".

Términos y condiciones de acceso y uso (Folios 201 a 203)

"CUARTO: TRATAMIENTO DE DATOS PERSONALES
4.1DEBER DE INFORMACIÓN
4.1.1 SENTINEL recopila, almacena, gestiona y administra los datos personales de EL USUARIO con la finalidad de validar la identidad de EL USUARIO y poder brindar el servicio que solicita.
4.1.2 SENTINEL declara que los datos personales de EL USUARIO serán tratados en cumplimiento con lo dispuesto en la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado por Decreto Supremo N° 003-2013-JUS.
4.1.3 Los datos personales de EL USUARIO serán tratados y almacenados en el Banco de Datos Personales de "Clientes" de SENTINEL, inscrito mediante Resolución N° 022-2015-JUS/DGPDP-DRN, ubicado en 4030 Lafayette Center Drive, 20151 Chantilly, Virginia, Estados Unidos de América y/o en Av. Javier Prado Este 6230, La Molina, Perú, por tiempo indefinido.
(…)
4.2 AUTORIZACIÓN DE TRATAMIENTO Y TRANSFERENCIA
4.2.1 EL USUARIO autoriza y otorga de manera libre, previa, expresa, inequívoca e informada su consentimiento a SENTINEL, para que éste pueda tratar los datos personales que EL USUARIO ingrese al registro "MI SENTINEL" con la siguiente finalidad:

• SENTINEL pueda enviarle correos electrónicos con información de riesgos (alertas de variación crediticia, barómetros u otro tipo de información).
• SENTINEL pueda enviarles ofertas comerciales, remitirles correos electrónicos, mensajes de textos y/o cualquier otra comunicación, que contenga publicidad, ofrecimiento de sus propios

servicios o productos. Por tal motivo, todas las comunicaciones efectuadas por SENTINEL a EL USUARIO, no constituyen SPAM según la Ley N° 28493, su Reglamento y modificatorias

4.2.2EL USUARIO autoriza y otorga de manera libre, previa, expresa, inequívoca e informada su consentimiento a SENTINEL, para que este último pueda transferir sus datos personales a las empresas debidamente identificadas como EMPRESAS ASOCIADAS, que se encuentran en el siguiente link: http://portal.sentinelperu.com/empresasasociadas.html, el cual EL USUARIO declara conocer y haber ingresado a dicho link, antes de aceptar los presentes términos y condiciones.
Estas empresas son previamente calificadas por SENTINEL, bajo requisitos y estándares de seguridad adecuados, las cuales se encuentran en constante actualización, con la finalidad de que dichas EMPRESAS ASOCIADAS puedan ofrecerle las ventajas y beneficios de sus propios servicios o productos o de terceros mediante cualquier comunicación (correo electrónico, mensaje de texto, llamadas, entre otros) que contenga publicidad.
(…). No otorgar su consentimiento para el tratamiento y transferencia prevista en esta cláusula no impedirá a EL USUARIO a recibir los servicios solicitados a SENTINEL y/o la contratación de los servicios de SENTINEL.
4.2.3Asimismo, EL USUARIO autoriza y otorga de manera libre, previa, expresa, inequívoca e informada su consentimiento a VERIFICA PERÚ S.A. (Empresa con domicilio en Avenida Salaverry N° 2375, distrito de San Isidro, Lima, dedicada a la recolección, análisis, sistematización, tratamiento y comercialización de información de marketing y/o datos personales, información para campañas de prospección comercial, selección de prospectos, consultorías y/o soluciones de marketing o mercadotecnia, captación de oportunidades de negocios, estudios de mercado, informes estratégicos, servicio de verificación domiciliaria y localización de personas), para que esta última pueda transferir sus datos personales a las empresas debidamente identificadas como EMPRESAS ASOCIADAS VERIFICA que se encuentran en el siguiente link: http://www.verificaperu.com/empresasasociadas.html, el cual EL USUARIO declara conocer y haber ingresado a dicho link, antes de aceptar los presentes términos y condiciones.
Estas empresas son previamente calificadas por VERIFICA PERÚ S.A., bajo requisitos y estándares de seguridad adecuados, las cuales se encuentran en constante actualización, con la finalidad de que éstas puedan ofrecerle las ventajas y beneficios de sus propios servicios o productos o de terceros mediante cualquier comunicación (correo electrónico, mensaje de texto, llamadas, entre otros) que contenga publicidad.(…). No otorgar su consentimiento para la transferencia prevista en esta cláusula no impedirá a EL USUARIO a recibir los servicios solicitados a SENTINEL y/o la contratación de los servicios de SENTINEL.
(…) (Subrayado propio)

71. Con fecha 23 de agosto de 2020, esta Dirección efectuó una revisión de oficio de la plataforma “Mi Sentinel” de la administrada (Folios 248 a 266), con fines de verificar si hubo variaciones sustanciales respecto a los documentos de obtención de consentimiento relacionados para el tratamiento de los datos personales de contacto que se recopila de los usuarios que se registren a la misma y que, de ser el caso, concretice una conducta de adecuación a la normativa de protección de datos personales.

72. Al respecto, este Despacho verificó que, para efectos de crear una cuenta de registro en “Mi Sentinel” el usuario debe marcar el recuadro habilitado que contiene la confirmación de lectura y aceptación de la Política de Privacidad (Folios 251 a 256) y Términos y Condiciones de “Mi Sentinel” (Folios 258 a 260), siendo que de la revisión de estos documentos, a diferencia de lo advertido por la DFI en su Informe Final de Instrucción ninguno de estos contiene una cláusula de tratamiento de datos personales para fines comerciales y publicitarios.

73.En tal sentido, se aprecia que la administrada tiene habilitados dos recuadros para ser marcados por el usuario de su sitio web que desea concluir con su registro en "Mi Sentinel" (Folio 250), para efectos de su registro en la plataforma, en el cual se muestra las siguientes opciones:

"□ He leído y acepto las **Políticas de Privacidad de Mi Sentinel** y además los **Términos y Condiciones de Mi Sentinel**.
□ He leído y otorgo mi Consentimiento para el **Tratamiento de datos personales**"

74. Sobre el contenido del documento de Política de Privacidad (Folios 251 a 256) este Despacho advierte de una interpretación conjunta de las cláusulas cuarta y quinta de dicho documento que la administrada estaría utilizando una fórmula encubierta de consentimiento automático para también recopilar y tratar datos personales distintos a aquellos que recopila a través del registro de un usuario en "Mi Sentinel" (siendo los datos recopilados por los formularios de registro únicamente N° DNI, digito verificador, correo electrónico y número de celular y/o móvil) a través de "*Terceros proveedores de servicios, darkweb, redes sociales, registros públicos y fuentes accesibles al público"* para destinarlos como insumo en la prestación de los servicios de Mi Sentinel (incluyéndose en este último la generación de reportes de crédito que también comercializa a terceros descritos en la cláusula 2.4 de la Política de Privacidad y en la cláusula 1.4. de los Términos y Condiciones)

En tal sentido las cláusulas cuarta y quinta referidas establecen lo siguiente:

*"**4. Información que Recolectamos y Procesamos***
Sentinel Perú S.A. como Responsable del Tratamiento, a través del aplicativo Mi Sentinel, así como a través de los Terceros proveedores de servicios, darkweb, redes sociales, registros públicos y fuentes accesibles al público, puede recopilar y tratar los siguientes datos:
- Fecha y hora del ingreso del Usuario.
- Tipo de documento de identidad del Usuario.
- Fecha de nacimiento.
- Nombres y apellidos del Usuario.
- Correo electrónico del Usuario.
- Teléfono celular del Usuario.
- Dirección del Usuario.
- Digito Verificador.
- Información de Riesgos del público en general, así como algunos datos que los hagan identificables.
(…)

5. Finalidades para el tratamiento de los datos personales de los Titulares
5.1. Finalidades para el tratamiento de los datos personales del Titular a favor de Sentinel Perú S.A.
El Usuario del aplicativo Mi Sentinel, reconoce que Sentinel Perú S.A. realizará el tratamiento de sus datos personales identificados en el numeral 4 de la presente Política, para las siguientes finalidades:
(i) Como insumo para que Sentinel Perú S.A. pueda prestar los servicios de Mi Sentinel.
(ii) El envío de mensajes de texto, correos electrónicos y correos físicos, con el propósito de medir la calidad del servicio, y para mantener al Titular actualizado sobre los servicios que ofrece y brinda Sentinel Perú S.A.
(iii) Permitir el acceso o utilización de la Información de Riesgos para la evaluación de solvencia económica de las personas que figuran en sus bases de datos de Sentinel Perú S.A., en su calidad de CEPIR, en concordancia con lo establecido en la Ley de Cepirs.
(iv) Contactarlo como Titular para actualizar la autorización y la presente Política.

(…)"
(Subrayado propio)

75.A criterio de esta Dirección, la fórmula de consentimiento empleada sería demasiado amplia y estaría facultando a Sentinel a recopilar y tratar la mayor cantidad posible de datos personales de identificación, *"así como algunos datos que los hagan identificables"* y datos de contacto para fines comerciales respecto a la generación de reportes de crédito, no cumpliendo con obtener un consentimiento expreso y libre por parte de su titular. Esto último al no darle la posibilidad al usuario a, en todo caso, manifestar su conformidad o no con cada una de las fuentes de obtención mencionadas (dicho sea de paso de manera amplia, sin siquiera especificar por cuáles se encontrarían conformadas y para qué tipo de datos en particular) en la cláusula cuarta *Terceros proveedores de servicios, darkweb, redes sociales, registros públicos y fuentes accesibles al público.*

76. Conforme ha sido desarrollado en considerandos previos, esta Dirección reitera que en ningún caso la información que fuera recopilada de fuentes de acceso al público habilitan al usuario de las mismas a incorporarlas en bancos de datos para un tratamiento y finalidad que no hubieran sido consentidos válidamente conforme lo establecido en la normativa de protección de datos personales.

77. Respecto al segundo recuadro de marcación habilitado por la administrada para que el usuario brinde consentimiento para el tratamiento de sus datos personales con fines comerciales y publicitarios, este Despacho advierte que la redacción de la leyenda que acompaña a dicho recuadro es inexacta *("He leído y otorgo mi Consentimiento para el* ***Tratamiento de datos personales****")* lo cual puede llevar fácilmente a inducir a error al usuario. Esto último, dado que no especifica que el consentimiento adicional que busca obtener del usuario, de estar éste de acuerdo, consiste en un consentimiento para el tratamiento de sus datos recopilados por Sentinel para fines comerciales y promocionales/publicitarios.

78.De la revisión del documento denominado "Consentimiento para el tratamiento de datos personales para acciones promocionales y conexas" (Folio 261) vinculado a este segundo recuadro implementado por la administrada, se aprecia que contiene la autorización para el tratamiento de los datos personales del usuario para ser transferidos a terceros con fines comerciales y publicitarios, conforme a seguir:

"Usted, Usuario del producto Mi Sentinel y titular de su Información personal, autoriza expresamente a Sentinel Perú S.A., a realizar el tratamiento de sus datos personales, identificados en el numeral 4 de la Política de Privacidad de Mi Sentinel, para que sean tratados en los términos expresados en la presente cláusula.

1. Finalidades
Usted otorga su consentimiento para que sus datos personales sean utilizados para los siguientes fines:
(i) Para que sean transferidos a Experian Perú S.A.C. con la finalidad de que –conjuntamente con Sentinel Perú S.A. – analice su riesgo crediticio con el propósito de determinar si es un sujeto apto para el otorgamiento de créditos por parte de terceros proveedores de servicios financieros (aliado o suscriptores de Experian Perú S.A.C.);
(ii) Para que Sentinel Perú S.A., Experian Perú S.A.C. y los Suscriptores y/o Aliados de Experian Perú S.A.C. puedan contactarlo para fines publicitarios, promocionales y/o comerciales, relacionados al ofrecimiento de sus productos y/o servicios.

(iii) Para diseñar y/o robustecer los programas de educación financiera y protección de datos de Sentinel Perú S.A.
(iv) Para que se le pueda ofrecer el programa "Buscacrédito" que, mediante el análisis, cruce y transferencia de su información con la base de datos de Sentinel Perú S.A., le indica qué entidades financieras (Suscriptores y/o Aliados de Experian Perú S.A.C.) le podrían ofrecer un producto o servicio financiero. Podrá encontrar todo el detalle, información y características del programa "Buscacrédito" en el siguiente link: https://buscacredito.experianconsumidor.com.pe/
(v) Para facilitar el registro en el programa "Buscacrédito" señalado en el numeral anterior, de manera que los datos de registro que el Usuario utilizó en Mi Sentinel, le sirvan para registrarse en "Buscacrédito" de manera más fácil, siendo trasladados dichos datos al registro de "Buscacrédito" una vez que el Usuario haya aceptado los Términos y Condiciones y la correspondiente Política de Privacidad de "Buscacrédito".
(…)" (Subrayado propio)

79. Por lo expuesto, este Despacho considera que la plataforma "Mi Sentinel" no constituye un medio idóneo de obtención de consentimiento válido por parte de sus usuarios.

80. En suma, respecto al análisis de las actuaciones de la administrada, este Despacho concluye que la misma no ha presentado acciones de enmienden totalmente la sanción a imponerse a la administrada por la responsabilidad incurrida de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP. Específicamente por haber realizado tratamiento de los datos personales de contacto trasferidos a CMAC Piura con fecha 6 de agosto de 2018, conforme la muestra revisada, sin haber obtenido válidamente el consentimiento de sus titulares que legitimen el tratamiento de los mismos para fines comerciales de Sentinel.

81. Cabe mencionar además, que las acciones realizadas serán tomadas en cuenta para la evaluación de la multa a imponerse, teniendo en cuenta que, dado que no es posible la acción de enmienda total de la infracción cometida, puesto que incluye la transferencia de datos a terceros, lo que implica que la información ha salido de la esfera de control de la administrada, no siendo posible retrotraer el hecho a una situación anterior al momento de cometida la infracción.

Sobre la determinación de las sanciones a aplicar

82.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.

83.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[36], sin perjuicio de las medidas correctivas que puedan determinarse de acuerdo con el artículo 118 del Reglamento de la LPDP[37].

84.En el presente caso, se ha establecido la responsabilidad de la administrada por recopilar y transferir a CMAC Piura S.A.C datos personales de contacto (números de celular, números de teléfono fijo y dirección) sin contar con el consentimiento de sus titulares. Obligación establecida en el artículo 13, numeral 13.5 de la LPDP; configurando 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 Nº 29733 y su Reglamento."*

84.Con el objeto de establecer las pautas y criterios para realizar el cálculo del monto de las multas aplicables por infracciones a la normativa de protección de datos personales en el ejercicio de la potestad sancionadora de la Autoridad Nacional de Protección de Datos Personales, mediante Resolución Ministerial N° 0326-2020-JUS, se aprobó la Metodología para el Cálculo de Multas en materia de Protección de Datos Personales[38].

85.Sobre la base de tal documento, se determinará el monto de la sanción a imponer por la infracción detectada.

86.Se ha determinado la comisión de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP, a la cual, de acuerdo con lo establecido en el inciso 2 del artículo 39 de la LPDP, corresponde una multa desde más de cinco (5) U.I.T. hasta cincuenta (50) U.I.T.

86.El beneficio ilícito ha resultado indeterminable, pues en el trámite del procedimiento administrativo sancionador no ha sido posible recabar medios probatorios que evidencien que el infractor haya obtenido o que espere obtener beneficios derivados de no cumplir con las disposiciones establecidas en materia de protección de datos personales, cometiendo la infracción; así como tampoco se tiene información sobre el monto que ahorra, ahorraría o pensaba ahorrar cometiendo la infracción (costos evitados).

---

[36] Ley N° 29733, Ley de Protección 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).
(…)

[37] **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.

[38] Documento disponible en: https://bnl.minjus.gob.pe/bnl/
Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.

87.En la medida que el beneficio ilícito resulta indeterminable, para determinar el monto de la multa corresponde aplicar la "multa prestablecida", cuya fórmula general es:

***M = Mb x F**, donde:*

M	Multa preestablecida que corresponderá aplicar en cada caso.
Mb	Monto base de la multa. Depende de la gravedad del daño del bien jurídico protegido: variable absoluta y relativa.
F	Criterios o elementos agravantes o atenuantes.

87.Bajo la fórmula de la multa prestablecida, el monto de la misma es producto del Monto Base (variable absoluta y la variable relativa) por los factores atenuantes o agravantes que se hayan presentado, conforme al inciso 3 del artículo 248 de la LPAG, así como los artículos 125 y 126 del Reglamento de la LPDP.

88.La variable absoluta da cuenta del rango en el que se encontraría la multa aplicable, dependiendo de si es una infracción muy grave, grave o leve. Por su parte, la variable relativa determina valores específicos dependiendo de la existencia de condiciones referidas al daño al bien jurídico protegido, como se aprecia en el siguiente gráfico:

Cuadro 2
Montos base de multas preestablecidas (Mb),
según variable absoluta y relativa de la infracción

Gravedad de la infracción	Multa UIT		Variable relativa y monto base (Mb)				
	Min	Máx	1	2	3	4	5
Leve	0.5	5	1.08	2.17	3.25		
Grave	5	50	7.50	15.00	22.50	30.00	37.50
Muy grave	50	100			55.00	73.33	91.67

89.Siendo que en el presente caso se ha acreditado la responsabilidad administrativa de la administrada conforme a la tipificación establecida en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP, corresponde el grado relativo "3", lo cual significa que la multa tendrá como Mb (Monto base) **22.50 U.I.T.**, conforme al siguiente gráfico:

N°	Infracciones graves	Grado relativo
2.b	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.	
	Datos No sensibles.	
	2.b.1. No pedir el consentimiento.	3
	2.b.2. Consentimiento no cumple con la característica de ser libre.	2
	2.b.3. Consentimiento no cumple con las demás características.	1
	Datos Sensibles.	
	2.b.4. No pedir el consentimiento.	4
	2.b.5. Consentimiento no cumple con la característica de ser libre.	3
	2.b.6. Consentimiento no cumple con las demás características.	2
	Datos Sensibles (salud y biométricos).	
	2.b.7. No pedir el consentimiento.	5

	2.b.8. Consentimiento no cumple con la característica de ser libre. 2.b.9. Consentimiento no cumple con las demás características.	4 3

Ahora bien, conforme a lo expuesto, el Mb debe multiplicarse por F, que es el valor atribuido a cada uno de los factores agravantes y atenuantes previstos en la normativa.

Cuadro 3

Valores de factores agravantes y atenuantes

f_n	Factores agravantes o atenuantes	Valor
f_1	**(d) Perjuicio económico causado**	
$f_{1.1}$	. No existe perjuicio.	0.00
$f_{1.2}$	. Existiría perjuicio económico sobre el denunciante o reclamante.	0.10
f_2	**(e) Reincidencia**	
$f_{2.1}$	. No hay reincidencia.	0.00
$f_{2.2}$	. Primera reincidencia.	0.20
$f_{2.3}$	. Dos o más reincidencias.	0.40

f_n	Factores agravantes o atenuantes	Valor
f_3	**(f) Las circunstancias**	
$f_{3.1}$	. Cuando la conducta infractora genere riesgo o daño a una persona.	0.10
$f_{3.2}$	. Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas.	0.20
$f_{3.3}$	. Cuando la conducta infractora haya afectado el interes público.	0.30
$f_{3.4}$	. Cuando la infracción es de carácter instantáneo y genera riesgo de afectación de otros derechos.	0.15
$f_{3.5}$	. Cuando la duración de la infracción es mayor a 24 meses.	0.25
$f_{3.6}$	. Entorpecimiento en la investigación y/o durante el procedimiento.	0.15
$f_{3.7}$	. Reconocimiento de responsabilidad expreso y por escrito de las imputaciones, después de notificado el inicio del procedimiento sancionador.	-0.30
$f_{3.8}$	. Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.	-0.15
$f_{3.9}$	. Colaboración con la autoridad, reconocimiento espontáneo y acción de enmienda, después de notificado el inicio del procedimiento sancionador.	-0.30
f_4	**(g) Intencionalidad**	
$f_{4.1}$	. Se advierte conocimiento y voluntad de cometer la conducta infractora	0.30

En el presente caso, de los medios probatorios que obran en el expediente no se verifica un perjuicio económico causado. Asimismo, la administrada no es reincidente.

El incumplimiento del artículo 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 persona, al no permitírsele decidir sobre el destino y acciones a efectuar con sus datos personales.

Del análisis del caso, y conforme a lo expuesto en la presente Resolución Directoral, en cuanto a las circunstancias de la infracción (f3), corresponde aplicarle las siguientes calificaciones para efectos del cálculo:

+0.20%, toda vez que la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas, puesto que se tomó una muestra de 22 personas, de las cuales en 20 se detectó la falta de consentimiento.

-15% toda vez que ha realizado acciones dirigidas a no cometer la infracción a futuro, acciones que no alcanzan a enmendar la infracción cometida, conforme lo desarrollado en la presente resolución.

En total, los factores de graduación suman un total de +5%, así como se muestra en el siguiente cuadro:

Factores de graduación	**Calificación**
f1. Perjuicio económico causado	0%
f2. Reincidencia	0%
f3. Circunstancias f3.2 Cuando la conducta infractora genere riesgo o daño a más de dos personas o grupo de personas f3.8 Colaboración con la autoridad y acción de enmienda parcial, después de notificado el inicio del procedimiento sancionador.	 20% -15%
f4. Intencionalidad	0
f1+f2+f3+f4	**5**

Considerando lo señalado anteriormente, luego de aplicar la fórmula prestablecida para el cálculo de la multa, el resultado es el siguiente:

Componentes	**Valor**
Monto base (Mb)	22.5 UIT
Factor de agravantes y atenuantes (F)	1.05
Valor de la multa	**23.63**

Por lo expuesto en el párrafo anterior, el valor final de la multa a imponer por la comisión de la infracción grave tipificada en el literal b), 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 esta Ley Nº 29733 y su Reglamento*" queda establecida en **veintitrés coma sesenta y tres unidades impositivas tributarias (23,63 UIT)**

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 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses aprobado por Decreto Supremo N° 019-2017-JUS;

SE RESUELVE:

Artículo 1.- Sancionar a SENTINEL PERÚ S.A. con la multa ascendente a veintitrés comas sesenta y tres unidades impositivas tributarias (23,63 UIT) por la comisión de la infracción grave tipificada en el literal b) del numeral 2 del artículo 132 del Reglamento de la LPDP.

Artículo 2.- Imponer como medida correctiva a SENTINEL PERÚ S.A. acreditar que ha eliminado y/o suprimido de los bancos de datos de su titularidad ("Información de Riesgos", "Clientes" y/o cualquier otro banco de datos que los contenga almacenados) los registros de datos personales de contacto (números telefónicos celulares/móviles y fijos y direcciones) que fueron materia de transferencia

Para el cumplimiento de tal medida correctiva, se otorga el plazo de cincuenta y cinco días hábiles (55) días hábiles contados a partir de la notificación de la presente resolución. En caso de presentar recurso impugnatorio el plazo para el cumplimiento de la medida correctiva es de treinta (30) días hábiles de notificada la resolución que resuelve el recurso y agota la vía administrativa.

Artículo 3.- Informar a SENTINEL PERÚ S.A. que el incumplimiento de la medida correctiva dispuesta en el artículo precedente 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[39]

Artículo 4.- Informar a SENTINEL PERÚ S.A 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[40].

Artículo 5.- Informar a SENTINEL PERÚ S.A que deberá realizar el pago de la multa en el plazo de veinticinco (25) días hábiles desde el día siguiente de notificada la presente Resolución.[41]

---

[39] **Artículo 132.- Infracciones**
Las infracciones a la Ley Nº 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.

[40] **Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nº 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."

[41] El pago de la multa puede ser realizado en el Banco de la Nación con el código 04759 o a la cuenta del Banco de la Nación: CTA.CTE R.D.R. N° 0000-281778 o CCI N° 01800000000028177801.

Artículo 6.- Informar a SENTINEL PERÚ S.A que en caso presente recurso impugnatorio, el plazo para pagar la multa es de diez (10) días hábiles de notificada la resolución que agota la vía administrativa, plazo que se contará desde el día siguiente de notificada dicha resolución que pone fin la vía administrativa.

Artículo 7.- Informar a SENTINEL PERÚ S.A**.** que se entenderá que cumplió con pagar la multa impuesta, si antes de que venzan los plazos mencionados, cancela el sesenta por ciento (60%) de la multa impuesta conforme a lo dispuesto en el artículo 128 del Reglamento de la LPDP[42]. Para el pago de la multa deberá considerar el valor de la UIT vigente al inicio de la fiscalización.

Artículo 10.- Notificar a SENTINEL PERÚ S.A la presente Resolución Directoral.

Regístrese y comuníquese.

Firmado por
GONZALEZ LUNA Maria Alejandra FAU 20131371617 hard

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

CN = GONZALEZ LUNA Maria Alejandra FAU 20131371617 hard
O = MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
OU = 20131371617
SerialNumber = PNOPE-42000734
Date: 07/07/2021 21:31

María Alejandra González Luna
Directora (e) de Protección de Datos Personales

[42] **Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo Nº 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."