"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

INFORME DE FISCALIZACIÓN Nº 112-2021-JUS/DGTAIPD-DFI-VAVM

A : **Olga María Escudero Vílchez**
Directora (e) de la Dirección de Fiscalización e Instrucción

De : **Vanessa Antonella Vargas Márquez**
Analista Legal de Fiscalización de la Dirección de Fiscalización e Instrucción

Asunto : Informar sobre las actuaciones de fiscalización realizadas en atención a la denuncia presentada contra **RISK CONSULTING S.A.C.**

Referencia : Fiscalización n.° 257-2020-DFI

Fecha : Miraflores, 03 de mayo de 2021.

El presente informe tiene como finalidad comunicar el resultado de la fiscalización realizada a **RISK CONSULTING S.A.C.**, en atención a la denuncia presentada por el señor Luis Eduardo Espinoza Villar (el denunciante), y de conformidad a las facultades de la Autoridad Nacional de Protección de Datos Personales establecidas en los numerales 17, 19 y 20 del artículo 33º[1] de la Ley n.° 29733, Ley de Protección de Datos Personales (en adelante, **LPDP**), y su reglamento aprobado por Decreto Supremo n.° 003-2013-JUS (en adelante, **RLPDP**), de conformidad a las funciones de la Dirección de Fiscalización e Instrucción señaladas en el artículo 75°[2] del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos aprobado por Decreto Supremo N° 013-2017-JUS.

I. ENTIDAD DENUNCIADA

- Nombre : **RISK CONSULTING S.A.C.**

[1] **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:
17. Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.
19. Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.
20. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

[2] **Artículo 75.- Funciones de la Dirección de Fiscalización e Instrucción**
b) Fiscalizar que el tratamiento de los datos personales que efectúen el titular o el encargado de tratamiento de datos personales cumplan las disposiciones técnicas que emita la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
c) Fiscalizar, de oficio o por denuncia de parte, los presuntos actos contrarios a lo establecido en la Ley de Protección de Datos Personales y su Reglamento.
d) Fiscalizar la transferencia del flujo transfronterizo de datos personales.

- D.N.I. : 20603633033
- Actividad económica : Principal – 6202 – Consultoría de informática y gestión de instalaciones
  Secundaria 1 – 6201 – Programación informática
- Dirección : Av. Javier Prado Este Nro. 488 Dpto. 20 Urb. Orquídeas
- Distrito : San Isidro
- Provincia : Lima
- Departamento : Lima

II. BASE LEGAL

- Constitución Política del Perú.
- Ley N° 29733, Ley de Protección de Datos Personales (LPDP).
- Decreto Legislativo N° 1353, Decreto Legislativo 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.
- Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales (RLPDP).
- Decreto Supremo N° 019-2017-JUS, Reglamento del Decreto Legislativo N° 1353.
- Decreto Supremo N° 013-2017-JUS, Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos.
- Resolución Directoral N° 019-2013-JUS/DGPDP, aprueba la Directiva de Seguridad de la Información.

III. ANTECEDENTES

1. El 16 de octubre de 2020, mediante correo electrónico dirigido a protegetusdatos@minjus.gob.pe ingresó la denuncia (f. 02 a 35) presentada por el señor Luis Eduardo Espinoza Villar, (en adelante, el denunciante) contra **RISK CONSULTING S.A.C.** (en adelante el denunciado).

En dicha denuncia manifiesta lo siguiente:

> *"Señores Autoridad Nacional de Protección de Datos Personales:*
>
> *Por medio del presente les envío un cordial saludo y adjunto el Formulario de denuncia por actos contrarios a la Ley 29733 y su Reglamento cometidos por la Empresa Risk Consulting S.A.C. y su dueño y Gerente General el colombiano Luis Ramiro Diaz Briceño.*
> *(…)*
> *La descripción de los hechos la transcribo a continuación:*
>
> *https://cdn.www.gob.pe/uploads/document/file/844197/FORMULARIO-DE-DENUNCIA-POR-ACTOS-CONTRARIOS.pdf*
>
> *El colombiano Luis Ramiro Diaz Briceño en el año 2018 constituyó la empresa Risk Consulting con RUC 20603633033, desde esa fecha viene comercializando un "software" denominado Inspektor, que es una base de datos de nombres de personas y empresas. Vende esa información proporcionando los datos*

confidenciales de las personas y empresas, alegando a sus clientes que esos datos los ayudará a conocer los antecedentes de las personas. A continuación, se envía el link del producto:

https://www.riskglobalconsulting.com/lstas-restrictivas.inspektor/

Inspektor es una base de datos de nombres de personas y empresas, por tanto la empresa Risk Consulting Perú no ha registrado su base de datos personales en el Registro Nacional de Protección de Datos Personales, esta atentando contra los derechos fundamentales de las personas pues vende la información de las personas argumentando que esta información les servirá para dar cumplimiento y conocer cuáles son los antecedentes de las personas, realiza el uso transfronterizo de la información peruana pues también la comercializa en su país natal Colombia y en otros países de Latinoamérica, no cuenta con el consentimiento de las personas para divulgar su información, comparte la información de las personas incumplimiendo medidas de seguridad. Finalmente, se solicite se cancele la base de datos de la empresa Risk Consulting por infringir la Ley 29733 y su Reglamento aprobado mediante Decreto Supremo 003-2013-JUS por los argumentos expuestos.

Atentamente,

Luis Espinoza".

Adjunta los siguientes documentos: Formulario de denuncia, Partida Registral Risk Consulting Perú, Vigencia de Poder Risk Consulting (junio 2020), RUC Risk Consulting Perú, Pasaporte Luis Diaz, Cédula Colombiano Luis Diaz, DNI Luis Espinoza, Contrato Inspektor Risk Consulting cambio seguro firmado y, evidencia uso de información de datos personas.

2. Mediante Oficio n° 1377-2020-JUS/DGTAIPD-DFI de 22 de diciembre de 2020 (f. 39 a 42), la Dirección de Fiscalización e Instrucción (DFI) requiere al denunciante lo siguiente:

- Adjunte evidencia referente al tratamiento de datos personales que realiza la denunciada a través del software denominado "Inspektor", así como qué datos personales son los que trataría de manera indebida, toda vez que de la documentación presentada no se logra advertir ello.

3. Mediante correo electrónico de fecha 01 de enero de 2021, el denunciante presenta documentación (f. 43 a 85).

4. El 18 de enero de 2021, mediante escrito ingresado por la mesa de partes con registro n.° 2021USC-051970, el denunciante absuelve el requerimiento solicitado mediante Oficio n.° 1377-2020-JUS/DGTAIPD-DFI (f. 86 a 127).

5. Mediante Carta n° 041-2021-JUS/DGTAIPD-DFI de 15 de febrero de 2021 (f. 128 a 135), la Dirección de Fiscalización e Instrucción (DFI) requiere a la empresa CAMBIO SEGURO FINTECH S.A.C. lo siguiente:

- Indique que datos personales trata a través del Software Inspektor. De ser el caso, especifique el tipo y, de qué manera accede a dicha consulta de datos personales. Adjunte evidencia (documentación, CD, video, etc.).

- Especifique cual es la finalidad por la que requiere la consulta de los datos personales en el Software Inspektor.
- Indique si el contrato de prestación de servicios de acceso consulta Inspektor de fecha 11 de agosto de 2020 se encuentra vigente.

6. Mediante Carta n° 042-2021-JUS/DGTAIPD-DFI de 15 de febrero de 2021 (f. 136 a 141), la Dirección de Fiscalización e Instrucción (DFI) requiere a la empresa SGS DEL PERU S.A.C. lo siguiente:

- Señale que datos personales trata a través del Software Inspektor. De ser el caso, especifique el tipo y, de qué manera accede a dicha consulta de datos personales. Adjunte evidencia (documentación, CD, video, etc.).
- Especifique cuál es la finalidad por la que requiere la consulta de los datos personales en el Software Inspektor.
- Indique si el contrato de servicios de fecha 14 de octubre de 2019 se encuentra vigente, toda vez que no se encuentra suscrito por Risk Consulting S.A.C.

7. Mediante Carta n° 043-2021-JUS/DGTAIPD-DFI de 15 de febrero de 2021 (f. 142 a 147), la Dirección de Fiscalización e Instrucción (DFI) requiere a la empresa TU CAMBISTA S.A.C. lo siguiente:

- Señale que datos personales trata a través del Software Inspektor. De ser el caso, especifique el tipo y, de qué manera accede a dicha consulta de datos personales. Adjunte evidencia (documentación, CD, video, etc.).
- Especifique cuál es la finalidad por la que requiere la consulta de los datos personales en el Software Inspektor.
- Indique si el contrato de prestación de servicios de fecha 15 de junio de 2020 se encuentra vigente, toda vez que no ha sido suscrito por la empresa Risk Consulting S.A.C.

8. Mediante Carta n° 044-2021-JUS/DGTAIPD-DFI de 15 de febrero de 2021 (f. 148 a 156), la Dirección de Fiscalización e Instrucción (DFI) requiere a la empresa TK BUSINESS ONLINE S.A.C. lo siguiente:

- Señale que datos personales trata a través del Software Inspektor. De ser el caso, especifique el tipo y, de qué manera accede a dicha consulta de datos personales. Adjunte evidencia (documentación, CD, video, etc.).
- Especifique cuál es la finalidad por la que requiere la consulta de los datos personales en el Software Inspektor.
- Indique si el contrato de prestación de servicios de acceso consulta Inspektor de julio de 2020 se encuentra vigente, toda vez que se advierte que no ha sido suscrito por la empresa Risk Consulting S.A.C. y tampoco hay una fecha exacta de suscripción del contrato.

9. El 22 de febrero de 2021, mediante escrito ingresado a la mesa de partes del MINJUS con registro nro. 031254-2021MSC, la empresa CAMBIO SEGURO FINTECH S.A.C. absuelve el requerimiento de información solicitado mediante Carta n.° 041-2021-JUS/DGTAIP-DFI. (f. 157 a 166).

10. El 23 de febrero de 2021, mediante escrito ingresado a la mesa de partes del MINJUS con registro nro. 031808-2021MSC, la empresa TU CAMBISTA S.A.C. absuelve el requerimiento de información solicitado mediante Carta n.° 043-2021-JUS/DGTAIP-DFI. (f. 167 a 177).

11. Mediante Proveído de 25 de febrero de 2021, esta Dirección dispuso ampliar el plazo de fiscalización a RISK CONSULTING SA.C. por cuarenta y cinco (45) días hábiles adicionales, los mismos que se contarán a partir del 02 de marzo de 2021 (f. 178 a 179).

12. Mediante Carta n° 070-2021-JUS/DGTAIPD-DFI de 25 de febrero de 2021 (f. 180 a 186), la Dirección de Fiscalización e Instrucción (DFI) requiere a la empresa RISK CONSULTING S.A.C. lo siguiente:

- Especifique que tipos de datos trata el software "INSPEKTOR" y, de qué manera obtiene dicha información. Adjunte evidencia (videos, CD, documentación, etc.).
- Señale si realiza el tratamiento de datos personales mediante dicho software, de ser afirmativa su respuesta, indique como obtiene dicha información y si cuenta con el consentimiento de los titulares de los datos personales. Adjunte evidencia.
- Identifique la entidad titular y/o encargada de la administración de la información que se encuentra en el software "INSPEKTOR".
- Especifique si el tratamiento de los datos personales contenidos en el software "INSPEKTOR" se encuentra a cargo de la empresa Risk Consulting S.A.C. o que otras empresas estarían relacionadas y/o vinculadas a dicha información. Adjunte evidencia.
- Indique dónde se encuentra ubicado el almacenamiento de la información recopilada a través de la página https://www.riskglobalconsulting.com/lstas-restrictivas.inspektor/ y el software "INSPEKTOR". Adjunte evidencia.
- Especifique las medidas de seguridad implementadas para el almacenamiento de la información en el software "INSPEKTOR". Adjunte evidencia.

13. Mediante Cédula de Notificación n° 153-2021-JUS/DGTAIPD-DFI de 25 de febrero de 2021 (f. 187 a 191), la DFI notifica al denunciante el Proveído de Ampliación de fecha 25 de febrero de 2021.

14. El 02 de marzo de 2021, mediante escrito ingresado a la mesa de partes del MINJUS con registro nro. 036788-2021MSC, la empresa TK BUSINESS ONLINE S.A.C. absuelve el requerimiento de información solicitado mediante Carta n.° 044-2021-JUS/DGTAIP-DFI. (f. 192 a 214).

15. El 10 de marzo de 2021, mediante escrito ingresado a la mesa de partes del MINJUS con registro nro. 043692-2021MSC, la empresa RISK CONSULTING S.A.C. absuelve el requerimiento de información solicitado mediante Carta n.° 070-2021-JUS/DGTAIP-DFI. (f. 215 a 530).

16. El 15 de abril de 2021, mediante escrito ingresado a la mesa de partes del MINJUS con registro nro. 2021USC-428842, la empresa SGS DEL PERU S.A.C. absuelve el requerimiento de información solicitado mediante Carta n.° 042-2021-JUS/DGTAIP-DFI. (f. 531 a 533).

17. Mediante Carta n° 156-2021-JUS/DGTAIPD-DFI de 26 de abril de 2021 (f. 534 a 539), la Dirección de Fiscalización e Instrucción (DFI) programa una fiscalización virtual a la empresa denunciada RISK CONSULTING S.A.C. para el día 28 de abril de 2021 a las 11:00 am.

18. El 26 de abril de 2021, mediante Orden de Fiscalización n.° 069-2021-JUS/DGTAIPD-DFI (f. 540 a 64), la Dirección de Fiscalización e Instrucción (DFI) de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD), en el marco de las actuaciones de fiscalización, de conformidad al artículo 33° de la LPDP, dispuso la realización de una de fiscalización virtual a la empresa denunciada RISK CONSULTING S.A.C. identificada con RUC n° 20603633033.

19. El 28 de abril de 2021, se realizó la única fiscalización virtual, dejándose constancia de los hechos en el Acta de Fiscalización n°. 01-2021 (f. 541 a 564).

IV. DETALLE DE LA FISCALIZACIÓN

20. En el Acta de Fiscalización n.° 01-2021 (f. 541 a 564), se registra lo siguiente (f. 542 a 545):

> *"(…)*
> *a. Se verificó que la administrada es propietaria de la aplicación "INSPEKTOR".*
> *b. La aplicación "INSPEKTOR" es de tipo web y para su acceso se requiere de usuario y contraseña; para acceder se realiza a través del URL: https://inspektor.datalaft.com/Default.aspx.*
> *c. La administrada informó que en la aplicación web cuentan con registros de personas naturales de distintos países.*
> *d. Se verificó que en la aplicación web "INSPEKTOR" cuentan con un registro aproximado de 829 876 personas naturales de nacionalidad peruana.*
> *e. La administrada informó que no cuenta con ningún banco de datos inscrito ante la ANPDP y tampoco se encuentra en proceso de inscripción.*
> *f. La administrada informó que el servidor físico que aloja los datos personales se encuentra en Colombia, asimismo, informó que no ha comunicado la realización de flujo transfronterizo.*
> *g. La administrada informó que la aplicación web es la presentación comercial del servicio que presta a las distintas entidades, dicho servicio es: brindar información de conocimiento público para facilitar el proceso de información en el marco del cumplimiento de la Política Nacional contra el Lavado de Activos y el Financiamiento del Terrorismo.*
> *h. La administrada informó que este servicio es brindado a distintas entidades con que mantiene una relación contractual y para su acceso se le brinda un usuario y contraseña de la aplicación "INSPEKTOR", la cual debe contar con ciertas características de seguridad, asimismo cuentan con una medida de seguridad denominada "Captcha".*

i. Se verificó que la aplicación web cuenta con un registro de consulta en la que se constató que cuenta con quien realizó la consulta, fecha y el resultado obtenido de ser el caso.
j. Se verificó que la aplicación "INSPEKTOR" cuenta con distintos módulos tales como cuenta configuración, notificaciones, consultar listas, lista propias y reportes
k. Se verificó que a través del módulo "consultar listas" se puede realizar una consulta de una persona natural ya sea por "nombres completos" o "documento de identificación". Asimismo, se verificó que como resultado de esta búsqueda arroja un "mapa de calor" de distintos colores, detallado en los anexos del presente documento denominado "resultados de la verificación de la aplicación - INSPEKTOR", a través del cual de manera preliminar se puede constatar los resultados del perfilamiento realizado al usuario consultado.
l. Respecto al "mapa de calor" la administrada informó que los resultados de la búsqueda son señalados en el color que corresponda y de acuerdo al nivel de riesgo que representa el usuario consultado.
m. La administrada informó que no cuentan con ningún tipo de contrato con alguna entidad pública que les brinde información respecto a los usuarios. Asimismo, informó que los datos de DNI o nombres completos son realizados a través de una consulta de la página WEB DE SUNAT.
n. La administrada informó que no cuenta con el consentimiento de los usuarios almacenados en la aplicación "INSPEKTOR" dado que se encuentra en el marco de la excepción del Art. 14 de la Ley No. 29733. Asimismo, informó que los datos que proporciona, son obtenidos de fuente de acceso al público, tales como:

- *ABC NOTICIAS Medio de Comunicación https://abcnoticias.pe/*
- *AGENCIA FISCAL Medio de Comunicación https://www.agenciafiscal.pe/*
- *ANCASH AL DIA Medio de Comunicación https://ancashaldia.com/*
- *ANCASH NOTICIAS Medio de Comunicación http://www.ancashnoticias.com/*
- *CHIMBOTE EN LINEA Medio de Comunicación http://www.chimbotenlinea.com/*
- *CONVOCA Medio de Comunicación http://convoca.pe/*
- *DIARIO CORREO Medio de Comunicación https://diariocorreo.pe/*
- *DIARIO DE CHIMBOTE Medio de Comunicación http://www.diariodechimbote.com/*
- *DIARIO OFICIAL EL PERUANO https://elperuano.pe/*
- *EL COMERCIO Medio de Comunicación https://elcomercio.pe/*
- *EL POPULAR Medio de Comunicación https://www.elpopular*

(…)
***Declaración del fiscalizado**:*
(…)
Como se mencionó nuestro servicio responde a un marco normativo extenso en el contexto internacional y nacional, en virtud del cual se han elevado los estándares de exigencia y responsabilidad del sector privado y que en conjunto constituyen parte esencial de herramientas de política criminal con una relevancia indiscutible en la lucha contra del Estado Peruano contra fenómenos como el lavado de activos, la financiación del terrorismo, la financiación de la proliferación de armas de destrucción masiva y la corrupción, y como tal posibilita a las organizaciones cumplir con sus obligaciones y participar de las políticas públicas para la prevención y lucha contra estos fenómenos.

Este desarrollo normativo en el contexto nacional advierte la necesidad de implementar sistemas de prevención y gestión de riesgos y de manera especial llaman la atención sobre la importancia de un adecuado "conocimiento de contrapartes/tercero" dentro de lo que se ha denominado "debida diligencia" y

"buena fe exenta de culpa" previo a cualquier relacionamiento y durante la vinculación. Este conocimiento cobija consulta en listas de información de naturaleza pública.
(…)
Desde RISK CONSULTING SAC y a través de la Plataforma INSPEKTOR se presta un servicio que permite a sus clientes cumplir con los requerimientos legales establecidos por las autoridades pertinentes, así como las mejores prácticas de manera que se implementen medidas eficientes para prevenir todos los riesgos asociados brindando información que se ha difundido a través de fuentes públicas y que posibilita la toma de decisiones bajo un enfoque de riesgo.

Se trata de un servicio integral a través de una herramienta tecnológica que automatiza y simplifica el acceso e interpretación de la información que es, a su vez, resultado de los procesos de investigación y análisis riguroso bajo estrictos estándares de calidad, a cargo de un equipo de analistas multidisciplinario con las más altas calidades técnicas y humanas.

*La información que se suministra a través de la Plataforma **INSPEKTOR** es el resultado del monitoreo y análisis de diversas fuentes de naturaleza pública, tales como medios de comunicación, páginas oficiales del Estado, listas nacionales o internacionales, entre otros; y aterrizado a las exigencias normativas (previamente señaladas). De las principales características a considerar en relación con la prestación del servicio **INSPEKTOR** y los "datos" o "información" que se suministra a sus clientes: (i) Se trata de una compañía cuyos procesos están certificados en calidad por la ISO 9001:2015; (ii) El trabajo que respalda nuestra plataforma es el resultado del esfuerzo, dedicación y empeño de un equipo multidisciplinario experto en análisis de riesgos; (iii) No se trata de Datos Sensibles en los términos del Artículo 2º numeral 5º de la Ley 29733 de 3 de Julio de 2011 de Protección de Datos Personales, pues no constituye ninguna de las categorías allí relacionadas; (iv) Se trata de información que reposa en fuentes públicas (por lo mismo no se provee información de antecedentes) y no requiere de consentimiento de ninguna clase. Y que conforme al contenido del Art. 14 de la Ley No. 29733 de 3 de Julio de 2011 de Protección de Datos Personales: "No se requiere el consentimiento del titular de datos personales para los efectos de su tratamiento en los siguientes casos (…) 2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público (…)"; y (v) El ingresar a un tercero en listas no supone un señalamiento positivo o negativo de ninguna clase. La interpretación o uso que se le da depende de los sistemas de gestión de riesgos de los usuarios del servicio y de acuerdo a los lineamientos normativos aplicables.*

La información es veraz, se ha actualizado y cumple con unos parámetros de calidad pero en todo caso puede ser rebatida o solicitarse su retiro o actualización a través de los canales dispuestos para ello y alineado con la normativa aplicable.

Es importante indicar que: (i) Previo a ingresar en algún país, se revisan los requerimientos normativos aplicables, especialmente los referentes a la Protección de Datos Personales, límites de acceso a la información, páginas de consulta y listas de interés; (ii) Se adecúan políticas y procesos de forma que se cumpla lo pertinente en cada jurisdicción; (iii) Se promueve la transparencia e integridad en las empresas/entidades (nuestro slogan es "Negocios Transparentes") y sirve de apoyo a las mismas (sector público o privado) para cumplir la ley.

(…)".

V. ANÁLISIS

A. SOBRE EL CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS PERSONALES

21. Respecto al consentimiento, la LPDP dispone lo siguiente:

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

22. El artículo 7° del RLPDP, establece que *"en atención al principio del consentimiento, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que este no sea expresado de forma directa como aquellas en las que se requiera presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones deberá manifestarse en forma expresa y clara.*

Por su parte, el artículo 12° del RLPDP establece los presupuestos bajo los cuales se otorga válidamente el consentimiento para el tratamiento de los datos personales:

1. Libre.
2. Previo.
3. Expreso e Inequívoco.
4. Informado.

23. El 16 de octubre de 2020, el señor Luis Eduardo Espinoza Villar denuncia que la empresa Risk Consulting S.A.C. viene comercializando un software denominado "Inspektor", el cual es una base de datos que contiene nombres de personas y empresas de carácter confidencial, alegando a sus clientes que esos datos los ayudará a conocer los antecedentes de las personas, asimismo, señala que la empresa denunciada no ha registrado su base de datos personales en el Registro Nacional de Protección de Datos Personales, así como tampoco el uso transfronterizo de la información peruana pues también la comercializa en su país natal Colombia y en otros países de Latinoamérica, no contando con el consentimiento de las personas para divulgar dicha información.

24. En atención a ello, esta Dirección de Fiscalización e Instrucción (DFI) cursó cartas a las empresas con las que mantiene una relación comercial como son: SGS DEL PERU S.A.C., TU CAMBISTA S.A.C, TK BUSINESS ONLINE S.A.C. y CAMBIO SEGURO FINTECH S.A.C. (f. 128 a 156), con el objetivo de verificar que datos personales son los que trata y con que finalidad realizan la consulta en el software "Inspektor", siendo que señalaron lo siguiente:

> *"(…)*
> *ingresamos el N° de DNI, Pasaporte, Carnet de Extranjería o RUC de nuestro cliente (el cual se registró previamente en nuestra web) así como su nombre completo; y descargamos el reporte generado por Inspektor, el cual indica si el cliente aparece en listas nacionales e internacionales relacionadas a los temas de prevención de lavado de activos y financiamiento del terrorismo (PLAFT)*
> *(…)*
> *Usamos el Software Inspektor para realizar el filtro PLAFT de nuestros clientes, dado que el Software nos permite consultar de forma automatizada las listas nacionales e internacionales requeridas por la Superintendencia de Banca y Seguros (SBS).*
> *(…)*
> *La finalidad de consultar a nuestros clientes en Inspektor, es cumplir con la* ***Resolución S.B.S. N° 789 – 20181****. En esta norma se solicita al sujeto obligado que, implemente un sistema de prevención contra el Lavado de Activos y Financiamiento del Terrorismo (LAFT), identificando a los clientes que necesitan estar bajo el Régimen Reforzado de Debida Diligencia en el Conocimiento del Cliente.*
>
> *Para que un cliente se encuentre en el régimen reforzado, se debe conocer si el cliente es una persona políticamente expuesta (PEP) o si es familiar de una PEP, se debe tener conocimiento si el cliente está siendo investigado por el delito de lavado de activos, delitos precedentes y/o financiamiento del terrorismo por las autoridades competentes, o si el cliente está vinculado con personas naturales o jurídicas sujetas a investigación o procesos judiciales relacionados con el lavado de activos, delitos precedentes y/o el financiamiento del terrorismo. Inspektor nos indica si la persona consultada se encuentra en alguna lista de riesgo internacional, y si así fuese, nos indica el nombre de la lista y el delito/cargo.*
> *(…)".*

25. El 10 de marzo de 2021 mediante escrito ingresado por mesa de partes con registro nro. 043692-2021MSC (f. 215 a 530), **RISK CONSULTING S.A.C**. señala lo siguiente (f. 232 a 244):

> *"(…)*
> *(…), el servicio que se ofrece por la empresa RISK CONSULTING S.A.C. no se restringe a temas LA/FT/FP ADM/CO. INSPEKTOR sirve como* ***una herramienta para el adecuado conocimiento de terceros que soporta la debida diligencia y sirve de complemento a modelos LA/FT pero también anticorrupción, modelos de prevención de delitos o incluso de simple cumplimiento normativo****, entre otros.*
>
> *El servicio se presenta entonces como "****servicio de acceso, consulta y verificación de información de Listas (restrictivas, informativas, y otras) que acompaña los procesos de "Debida Diligencia" (general y reforzada) para el***

conocimiento del cliente, directores, trabajadores, proveedores y contrapartes en general*" y no como falsamente lo señala el denunciante para "conocer antecedentes" (información que para el caso peruano no se tiene por ser información sujeta a reserva).*

Se trata de un servicio integral a través de una herramienta tecnológica que automatiza y simplifica el acceso e interpretación de la información que es, a su vez, resultado de los procesos de investigación y análisis riguroso bajo estrictos estándares de calidad, a cargo de un equipo de analistas multidisciplinario con las más altas calidades técnicas y humanas.

Es importante reiterar que esta obligación la deben cumplir las empresas, pero desde el plano operativo sería una carga muy pesada ingresar a cada plataforma, cada lista y finalmente abordar todos los resultados que ofrecen buscadores como google, permitiendo esta herramienta que en apenas 2 segundos traiga extractada la información y ya habiendo depurado falsas noticias, información errada, antitécnica, información desactualizada o hallazgos de homónimos o similares

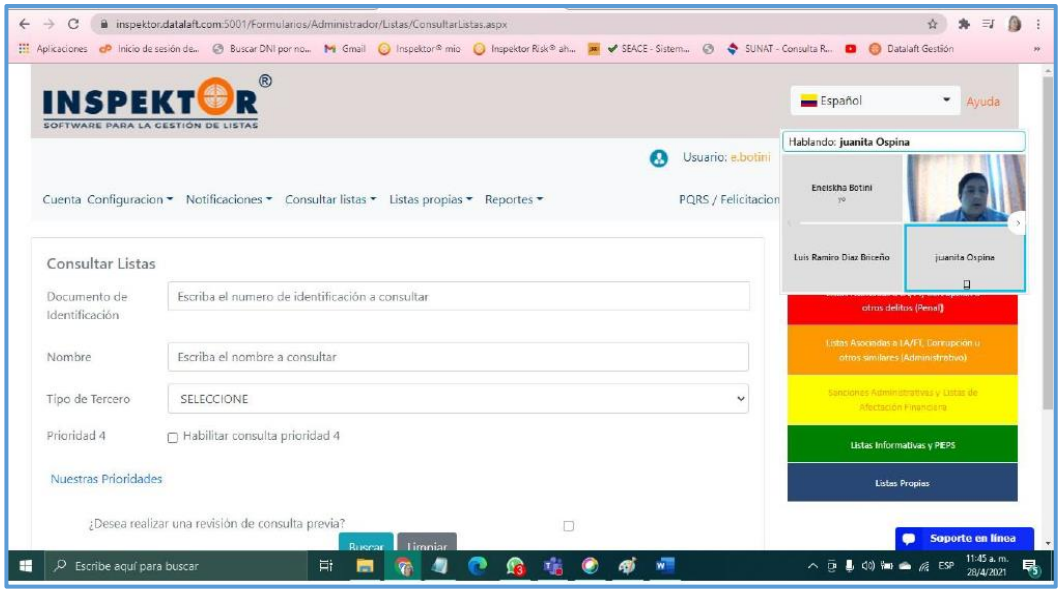
Es un servicio privado que se adquiere con el propósito de cumplir con la obligación de adelantar procesos de conocimiento de terceros y debida diligencia, permitiendo simplificar consultas que harían directamente en fuentes abiertas unificando el resultado y ofreciendo respuesta en pocos segundos.

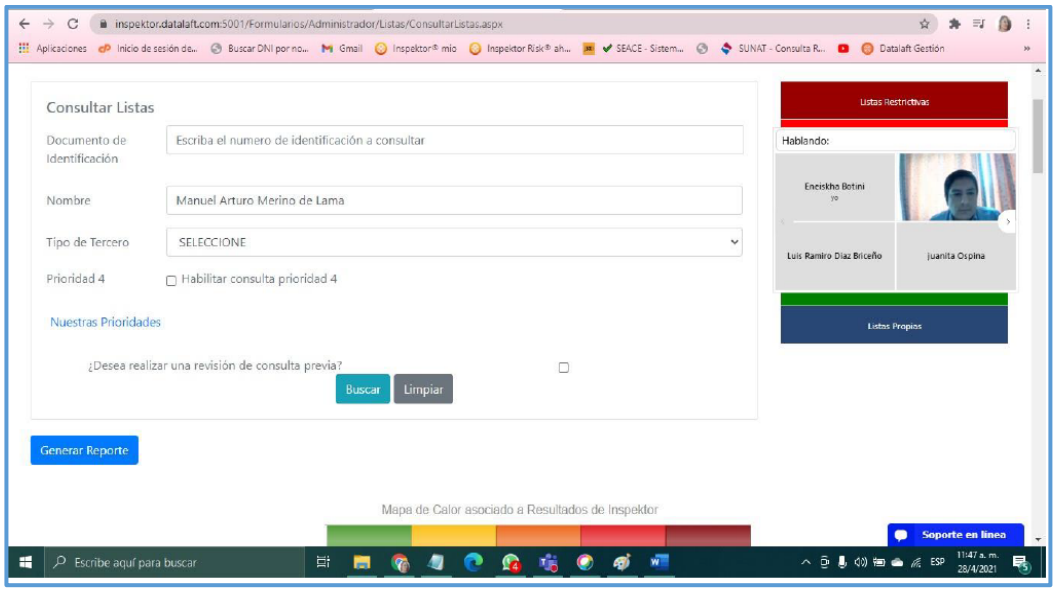
La información que sirve de soporte o consulta en la herramienta Inspektor, únicamente integra datos personales que se encuentran en fuentes públicas y no se ingresa información alguna que tenga restricción o limitación de acceso o conocimiento, o que requiera de autorización del titular en aplicación de la normativa pertinente*.*
(…)
Toda la información de donde se toman los datos ingresados proviene de fuentes públicas lo que incluye- entre otros- medios de comunicación. Para ello se hace un filtro de fuentes buscando que se trate de fuentes serias, con reconocimiento, se trate de información que tiene réplica o difusión en otras fuentes, y en todo caso se busca complementar la información con registros de fuentes oficiales *(p.e. Ministerio Público).*
(…)
No se realiza tratamiento de datos sensibles en los términos del Artículo 2º numeral 5º de la Ley 29733 *de 3 de Julio de 2011 de Protección de Datos Personales, pues no constituye ninguna de las categorías allí relacionadas;* ***Considerando que se trata de información que reposa en fuentes públicas, y no se trata de información que aporte o provea el titular de la información, y en aplicación del Art. 14 de la Ley No. 29733*** *de 3 de Julio de 2011 de Protección de Datos Personales "****No se requiere el consentimiento del titular de datos personales para los efectos de su tratamiento en los siguientes casos (…) 2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público (…)".***
(…)".
(Lo resaltado es nuestro).

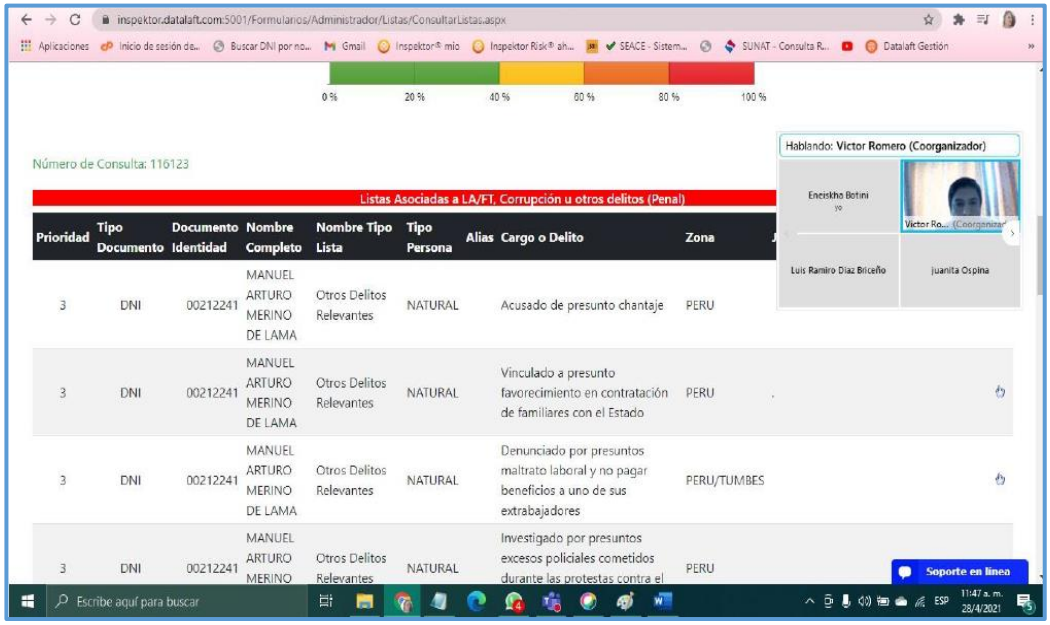
26. Sobre el tratamiento de datos personales, la LPDP lo define en el artículo 2°, numeral 19 como *"cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización,*

bloqueo, supresión, comunicación por transferencia, o por difusión o por cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales".

27. Al respecto, las actuaciones de fiscalización constataron a través del Acta de fiscalización n° 01-2021-DFI que la denunciada realiza tratamiento de datos personales (nombres, apellidos y D.N.I.) a través del software "Inspektor", contando con un registro aproximado de 829 876 personas naturales de nacionalidad peruana, asimismo, la denunciada alegó que no cuenta con el consentimiento de los usuarios de los datos personales almacenados en dicho software "Inspektor", indicando que se encuentra en el marco de la excepción del artículo 14° de la Ley de Protección de Datos Personales - Ley Nro. 29733, ya que los datos que proporciona son obtenidos de fuente de acceso al público.







Prioridad	Tipo Documento	Documento Identidad	Nombre Completo	Nombre Tipo Lista	Tipo Persona	Alias	Cargo o Delito	Zona
3	DNI	00212241	MANUEL ARTURO MERINO DE LAMA	Otros Delitos Relevantes	NATURAL		Acusado de presunto chantaje	PERU
3	DNI	00212241	MANUEL ARTURO MERINO DE LAMA	Otros Delitos Relevantes	NATURAL		Vinculado a presunto favorecimiento en contratación de familiares con el Estado	PERU
3	DNI	00212241	MANUEL ARTURO MERINO DE LAMA	Otros Delitos Relevantes	NATURAL		Denunciado por presuntos maltrato laboral y no pagar beneficios a uno de sus extrabajadores	PERU/TUMBES
3	DNI	00212241	MANUEL ARTURO MERINO	Otros Delitos Relevantes	NATURAL		Investigado por presuntos excesos policiales cometidos durante las protestas contra el	PERU

28. Ahora bien, con respecto a lo manifestado, el numeral 2, del artículo 14° de la LPDP, establece que no se requiere el consentimiento del titular de los datos personales: "*cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público*".

29. Sobre el particular, el numeral 11 del artículo 2° de la LPDP define a las fuentes accesibles al público como *"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 al público son determinadas en el reglamento"*.

30. Al respecto, sobre el uso de los datos obtenidos de fuentes accesibles al público, la DGTAIPD mediante el Oficio n° 749-2018-JUS/DGTAIPD del 07 de agosto de 2018 absuelve una consulta indicando *"(…) los datos contenidos en fuentes de acceso al público deben utilizarse únicamente para las finalidades para las cuales los datos personales son puestos a disposición en dichas fuentes. En ese marco, para finalidades distintas se debe requerir el consentimiento del titular de los datos personales, tales como ofrecimiento de bienes y servicios".*
(…)

Por lo tanto, 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 ese sentido, para incluir datos personales obtenidos de fuentes de acceso al público en bases de datos que van a ser comercializadas, se debe obtener de forma previa el consentimiento de los titulares de los datos personales. Al respecto, el artículo 13, inciso 13.9 de la LPDP establece que la comercialización de datos personales contenido o destinados a ser contenidos en bancos de datos personales se sujeta a los principios previstos en la LPDP (…)".

31. En cuanto a la cuestión alegada de que los datos que recopila el software "Inspektor" están contenidos en fuentes abiertas accesibles al público como es los medios de comunicación, páginas oficiales del Estado, listas nacionales e internacionales, debe precisarse que si bien califica como una fuente de acceso al público según los numerales 1 y 3 el artículo 17° del RLPDP[3], el último párrafo del citado artículo precisa que el tratamiento de los datos personales obtenidos a través de fuentes de acceso público deberán respetar los principios establecidos en la LPDP y su reglamento, entre los que figura el consentimiento, por lo que para el tratamiento de los datos personales recogidos en una base de datos con finalidades de comercialización, se requiere del consentimiento del titular de los datos personales, lo cual en el presente caso, no habría ocurrido.

32. No obstante, cabe precisar que la DGTAIP mediante el Oficio n° 749-2018-JUS/DGTAIPD del 07 de agosto de 2018 señala lo siguiente *"(…) El artículo 14° de la LPDP establece de forma expresa dos excepciones a la obligación de solicitar el consentimiento referidas al lavado de activos:*

> *"**Articulo 14 Limitaciones al consentimiento para el 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*

[3] **Artículo 17.- Fuentes accesibles al público.**
Para los efectos del artículo 2, inciso 9) de la Ley, se considerarán fuentes accesibles al público, con independencia de que el acceso requiera contraprestación, las siguientes:
1. Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.
2. Las guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica.
3. Los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica.
4. Los medios de comunicación social.
5. Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo.
En el caso de colegios profesionales, podrán indicarse además los siguientes datos de sus miembros: número de colegiatura, fecha de incorporación y situación gremial en relación al ejercicio profesional.
6. Los repertorios de jurisprudencia, debidamente anonimizados.
7. Los Registros Públicos administrados por la Superintendencia Nacional de Registros Públicos - SUNARP, así como todo otro registro o banco de datos calificado como público conforme a ley.
8. Las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública.
Lo dispuesto en el numeral precedente no quiere decir que todo dato personal contenido en información administrada por las entidades sujetas a la Ley de Transparencia y Acceso a la Información Pública sea considerado información pública accesible. La evaluación del acceso a datos personales en posesión de entidades de administración pública se hará atendiendo a las circunstancias de cada caso concreto.
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.

Unidad de Inteligencia Financiera, que estas puedan compartir información entre si 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.

33. Al respecto, lo que la normativa nos señala es que no se requiere del consentimiento del titular del dato personal cuando la finalidad es para el cumplimiento de las normas vinculadas al sistema de prevención de lavado de activos y financiamiento del terrorismo, lo cual se basa en que las empresas que se encuentran obligadas a informar a la Unidad de Inteligencia Financiera deben brindar información de sus clientes para prevenir el lavado de activos y financiamiento del terrorismo como información preventiva; sin embargo, para finalidades distintas se deberá de solicitar el consentimiento, lo cual no ocurre en el presente caso, ya que la denunciada no es sujeto obligado de informar.

34. Cabe precisar, que la denunciada a través del software "Inspektor" tiene como finalidad el brindar el servicio de acceso a bases de datos de lista de personas naturales y/o jurídicas relacionadas con delitos de lavados de activos y financiación del terrorismo, corrupción u otros delitos relevantes en materia de gestión de riesgo, lo cual corresponde a una finalidad comercial.

35. Las bases de datos correspondiente a Perú con las que cuenta el software "Inspektor" son:

"Listas Nacionales
- *Lista 80: Perú - Registro de Personas Sancionadas por el Estado Peruano;*
- *Lista 83: Perú - Los Peruanos de Lava Jato;*
- *Lista 94: Perú - Abogados Sancionados;*
- *Lista 105: Perú - Personas sancionadas por la Superintendencia de Banca y Seguros;*
- *Lista 113: Perú - Panama Papers y las Investigaciones del Ministerio Público de Perú;*
- *Lista 114: Perú - Investigados y Condenados por el Poder Judicial Perú;*
- *Lista 116: Perú-Contribuyentes excluidos del Régimen de Buenos contribuyentes;*
- *Lista 117: Perú-Proveedores Sancionados por el Tribunal de Contrataciones del Estado;*
- *Lista 118: Perú - Listados de Sujetos comprendidos en la Categoría 1 de la Ley N° 30737;*
- *Lista 122: Perú - Registro de Sanciones por Responsabilidad Administrativa Funcional a cargo de la Contraloría;*
- *Lista 123; Perú- Contribuyentes en condición No Hallados y No Habidos SUNAT;*
- *Lista 124: Perú- Derechos Mineros que no cumplieron con el pago oportuno del derecho de vigencia y/o penalidad;*
- *Lista 125: Perú - Relación de Buenos Contribuyentes Perú*
- *Lista 126: Perú- Registro "Mira a quién le compras" de sanciones aplicadas por el INDECOPI;*
- *Lista 130: Perú-Mas buscados del Perú;*
- *Lista 164: Perú- Registro para personas jurídicas sancionadas- Registro Nacional Judicial RENAJU*

(En construcción);
- *Lista 206: Perú - Empresas Sancionadas por la Superintendencia Nacional de Fiscalización Laboral*
- *Listas Peps*
- *Locales:*

▪ *Lista 73: Perú - Personas Políticamente Expuestas (Resolución SBS N° 4349-2016)*
▪ *Lista 74: Perú - PEPs en dejación del cargo (Resolución SBS N° 43492016)*
Relacionados:
▪ *Lista 170: Perú- Relacionados directos PEPs (Familiares y Organizaciones privadas en que participa) (En Construcción)*
(…)

36. Respecto al consentimiento y la carga de la prueba, el artículo 15° del RLPDP, dispone *"Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley y en el presente reglamento, la carga de la prueba recaerá en todos los casos en el titular del banco de datos personales o quien resulte responsable del tratamiento"*.

37. En el presente caso, se ha verificado que la denunciada a través del software "Inspektor" brinda el servicio de acceso a bases de datos de personas de nacionalidad peruana sin obtener el consentimiento de los titulares de los datos personales, lo cual evidenciaría que se ha realizado el tratamiento de los datos personales sin el consentimiento del titular de los datos personales, por tanto debe considerarse incumplido el principio de consentimiento regulado en el artículo 5° de la LPDP, así como lo señalado en el artículo 13°, numeral 13.5 de la citada norma.

38. En ese sentido, de las acciones de fiscalización efectuadas se ha determinado que la denunciada presumiblemente habría efectuado tratamiento de datos personales a través del software "Inspektor" sin el consentimiento de los titulares de los datos personales, hecho que podría configurar una presunta infracción grave, según lo regulado en el literal b, numeral 2, artículo 132° del RLPDP, esto es, *"dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley n° 29733 y su Reglamento"*.

C. INSCRIPCIÓN EN EL REGISTRO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

C.1. Banco de datos personales

39. Las actuaciones de fiscalización constataron a través del Acta de Fiscalización n° 01-2021-DFI, que la fiscalizada realiza tratamiento de datos personales a través del software "Inspektor" de personas naturales de nacionalidad peruana con un registro aproximado de 829 876, por lo que contaría con un banco de datos personales de **personas analizadas**[4]; sin embargo, no cuenta con ningún banco inscrito ante ANPDP y tampoco se encuentra en proceso de inscripción (f. 542).

40. Asimismo, por la actividad económica que realiza, es decir la actividad de consultoría informática y gestión de instalación informática contaría con el banco de datos personales de **clientes** y **proveedores**. Respecto a la consulta del RUC

[4] Lista de personas naturales relacionadas con delitos de lavado de activos y financiación del terrorismo, corrupción u otros delitos relevantes en materia de gestión de riesgo

de la fiscalizada se observa que en la declaración realizada a la SUNAT no cuenta actualmente con trabajadores en el periodo 02-2021, tal como se muestra en la siguiente captura de pantalla:

CANTIDAD DE TRABAJADORES Y/O PRESTADORES DE SERVICIO DE 20603633033 - RISK CONSULTING S.A.C.

Información de Trabajadores y/o Prestadores de Servicio

La información mostrada a continuación corresponde a lo declarado por el contribuyente en la Planilla Electrónica o PLAME ante la SUNAT. La información presentada corresponde a los 12 últimos períodos vencidos al mes anterior al día de la consulta.

Período	N° de Trabajadores	N° de Pensionistas	N° de Prestadores de Servicio
2020-04	1	0	5
2020-05	1	0	3
2020-06	1	0	4
2020-07	1	0	3
2020-08	1	0	0
2020-09	1	0	0
2020-10	1	0	0
2020-11	0	0	2
2020-12	0	0	4
2021-01	0	0	2
2021-02	0	0	3
2021-03	0	0	2

41. Finalmente, se observa que si bien en el software "Inspektor" no figura un formulario de libro de reclamaciones; sin embargo, por la actividad principal que realiza y los posibles reclamos o quejas de los clientes, debería de tener a disposición un libro de reclamaciones en su domicilio fiscal, ello de conformidad a lo señalado en el artículo 150° del Código de Protección y Defensa del Consumidor[5], por lo que contaría con un banco de datos de **libro de reclamaciones.**

42. El artículo 34° de la LPDP, establece que serán objeto de inscripción en el Registro Nacional de Protección de Datos Personales, los bancos de datos personales de administración privada.

43. El artículo 78° del RLPDP dispone que *"Las personas naturales o jurídicas del sector privado o entidades públicas que creen, modifiquen o cancelen bancos de datos personales están obligadas a tramitar la inscripción de estos actos ante el Registro Nacional de Protección de Datos Personales".*

44. De la consulta al Registro Nacional se verifica que la administrada ha inscrito los siguientes bancos de datos personales:

[5] **Código de Protección y Defensa del Consumidor**
Artículo 150.- Libro de reclamaciones
Los establecimientos comerciales deben contar con un libro de reclamaciones, en forma física o virtual. El reglamento establece las condiciones, los supuestos y las demás especificaciones para el cumplimiento de la obligación señalada en el presente artículo.

- Mediante Resolución Directoral N° 382-2017-JUS/DGPDP-DRN se inscribió el Banco de datos personales denominado **PROVEEDORES** código RNPDP-PJP n.° 11948.

- Mediante Resolución Directoral N° 383-2017-JUS/DGPDP-DRN se inscribió el Banco de datos personales denominado **POSTULANTES** código RNPDP-PJP n.° 11949.

- Mediante Resolución Directoral N° 384-2017-JUS/DGPDP-DRN se inscribió el Banco de datos personales denominado **COLABORADORES** código RNPDP-PJP n.° 11950.

45. Por lo tanto, se advierte que la administrada no habría inscrito ante el Registro Nacional de Protección de Datos Personales los bancos de datos personales de **personas analizadas, clientes (personas naturales)** y **libro de reclamaciones** detectados en la presente fiscalización, hecho que calificaría como una presunta infracción según lo señalado en el **literal e, numeral 1, artículo 132° del RLPDP**: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley".*

C.2. Comunicación de flujo transfronterizo de datos personales

46. Las actuaciones de fiscalización constataron a través del Acta de Fiscalización n° 01-2021-DFI, que la fiscalizada realiza tratamiento de datos personales a través del software "Inspektor" de personas naturales de nacionalidad peruana con un registro aproximado de 829 876 (f.542).

47. Asimismo, la fiscalizada informó que el servidor físico que aloja la información del software "Inspektor" se encuentra ubicado en Colombia, lo cual implica la realización de flujo transfronterizo de los datos personales recopilados (f. 542).

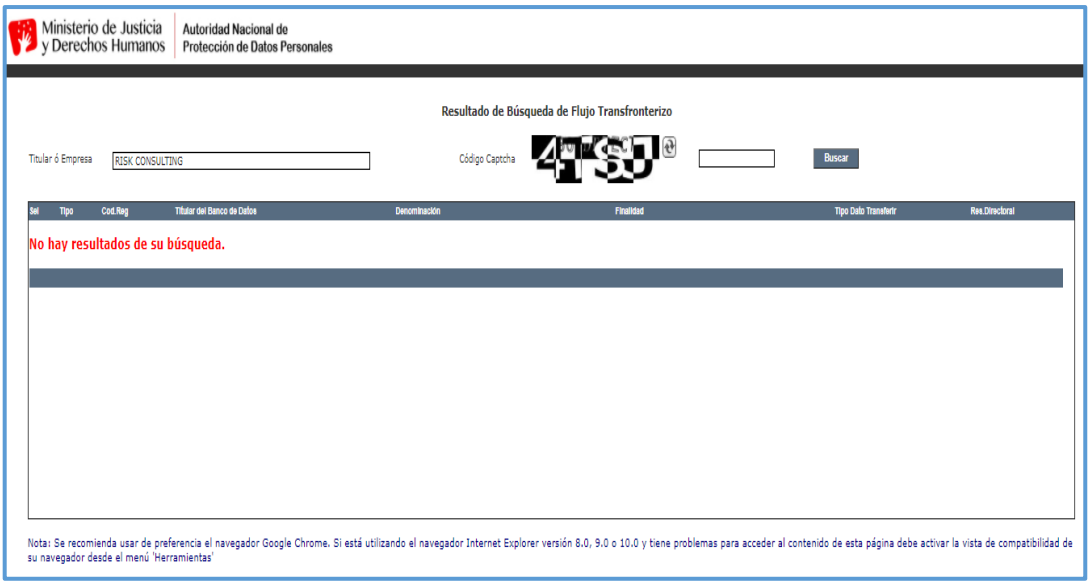
48. El numeral 10 del artículo 2° de la LPDP define al flujo transfronterizo de datos personales como la *"Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban".*

49. Asimismo, el numeral 18° del mismo texto normativo, define a la transferencia de datos personales como *"Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales".*

50. El artículo 26° del Reglamento de la LPDP establece que el flujo transfronterizo de datos personales se pondrá en conocimiento de la Dirección General de Protección de Datos Personales (hoy Dirección General de Transparencia, Acceso a la Información Pública y Datos Personales).

51. A su vez, el artículo 34° de la LPDP contempla como actos inscribibles ante el Registro Nacional de Protección de Datos Personales, las comunicaciones de flujo transfronterizo de datos personales, en concordancia con el numeral 5 del artículo 77° del Reglamento de la LPDP.

52. En atención a lo expuesto, esta Dirección procedió a ingresar al sistema web del Registro Nacional de Protección de Datos Personales, constatando que no figura inscrita comunicación de flujo transfronterizo, tal como consta en la siguiente captura de pantalla:



53. De lo expuesto, se evidencia que la fiscalizada no ha cumplido con inscribir ante el Registro Nacional la comunicación de flujo transfronterizo de los datos personales recopilados a través del software "Inspektor", toda vez que el servidor se encuentra localizado en el país de Colombia, el hecho señalado constituiría una presunta **infracción leve** según el **literal e., numeral 1, del artículo 132° del Reglamento de la LPDP**: "No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34° de la Ley".

54. El hecho señalado constituiría una presunta **infracción leve** según el **literal e., numeral 1, del artículo 132° del Reglamento de la LPDP**: "No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34° de la Ley".

V. ATENUANTES

55. De acuerdo al artículo 126° del Reglamento de la LPDP, constituye atenuante la colaboración del administrado con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones, acompañado de acciones de enmienda; lo que, atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda permitirá la reducción motivada de la sanción por debajo del rango previsto en la Ley.

VI. CONCLUSIONES Y RECOMENDACIONES

Primera.- RISK CONSULTING S.A.C. identificada con **R.U.C. n° 20603633033,** estaría realizando tratamiento de datos personales sin haber obtenido el consentimiento de los titulares de datos conforme a lo señalado en el artículo 13.5 del artículo 13° de la LPDP, y el artículo 12 del Reglamento de la LPDP. Hecho que constituiría una presunta infracción, según lo regulado en el literal b, numeral 2, artículo 132° del Reglamento de la LPDP, esto es, *"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",* dicha infracción es **grave** conforme al citado artículo.

Recomendación: Para usar los datos con fines comerciales debe contar con el consentimiento de los titulares, cumpliendo con las características dispuestas en el artículo 12° del Reglamento de la LPDP.

Segunda.- RISK CONSULTING S.A.C, no habría inscrito en el Registro Nacional de Protección de Datos Personales los bancos de datos personales de **personas analizadas, clientes (personas naturales)** y **libro de reclamaciones** detectados en la fiscalización. Hecho que constituiría una presunta infracción de conformidad con el **literal e, numeral 1, artículo 132° del RLPDP**: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley",* dicha infracción es **leve** conforme al citado artículo.

Recomendación: Inscribir ante el Registro Nacional de Protección de Datos Personales los bancos de datos personales detectados en la presente fiscalización[6].

Tercera.- RISK CONSULTING S.A.C., no habría comunicado a la Dirección General de Transparencia Acceso a la Información Pública y Protección de Datos Personales, para su inscripción en el Registro Nacional el flujo transfronterizo que realiza de los datos personales recopilados a través de su software "Inspektor". Hecho que constituiría una presunta infracción de conformidad con el literal e. del numeral 1 del artículo 132° del Reglamento de la LPDP: *"No inscribir o actualizar en el Registro Nacional los actos establecidos en el artículo 34 de la Ley",* dicha infracción es **leve** conforme al citado artículo.

Recomendación: Inscribir ante el Registro Nacional de Protección de Datos Personales el flujo transfronterizo de los datos de los usuarios del sitio web que realiza hacia Colombia.[7]

---

[6] Completar el formulario **INSCRIPCIÓN DE BANCO DE DATOS PERSONALES PERSONA JURÍDICA** que se encuentra publicado en el sitio web https://www.gob.pe/minjus con el siguiente enlace: https://www.minjus.gob.pe/wp-content/uploads/2018/12/FORMULARIO-DE-INSCRIPCI%C3%93N-DE-BDP-PERSONA-JUR%C3%8DDICA.pdf. Revisar la **GUÍA DE INSCRIPCIÓN DE BANCO DE DATOS PERSONALES** que se encuentra publicado en el sitio web https://www.gob.pe/minjus con el siguiente enlace: https://www.minjus.gob.pe/wp-content/uploads/2014/09/Cartilla-Registro-NEW-BAJA.pdf.

[7] Completar el formulario el **FORMULARIO DE INSCRIPCIÓN DE COMUNICACIÓN DE REALIZACIÓN DE FLUJO TRANSFRONTERIZO DE DATOS PERSONALES (TRANSFERENCIA INTERNACIONAL)** publicado en el sitio web https://www.gob.pe/minjus con el siguiente enlace:

Se hace de conocimiento de la fiscalizada que de realizar las acciones de enmienda recomendadas, deberá comunicar su implementación a la Dirección de Fiscalización e Instrucción mediante escrito presentado a través del Formulario de Mesa de Partes Virtual (MPV), el cual se encuentra ubicado en el link https://sgd.minjus.gob.pe/sgd-virtual/public/ciudadano/ciudadanoMain.xhtml, es necesario indicar que el horario de atención de la MPV es de lunes a viernes de 08:00 a 18:00 horas, así como que los envíos fuera de horario serán registrados a las 08:00 horas del día hábil siguiente, a fin de evitar el inicio de un procedimiento administrativo sancionador[8].

Asimismo, ante la contingencia sanitaria que se encuentra inmerso nuestro país y el ordenamiento de emergencia sanitaria y aislamiento social emitida por el Estado a nivel nacional, es necesario que la administrada señale como domicilio procesal un **correo electrónico para futuras notificaciones**, ello de conformidad a lo establecido en el numeral 20.4 del artículo 20° del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 004-2019-JUS[9].

---

https://www.minjus.gob.pe/wp-content/uploads/2018/12/Formulario-de-inscripci%C3%B3n-de-comunicaci%C3%B3n-de-realizaci%C3%B3n-de-flujo-transfronterizo-de-datos-personales.pdf

[8] **TEXTO ÚNICO ORDENADO DE LA LEY N° 27444, LEY DE PROCEDIMIENTO ADMINISTRATIVO GENERAL, APROBADO POR DECRETO SUPREMO N° 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.

[9] **TEXTO ÚNICO ORDENADO DE LA LEY N° 27444, LEY DE PROCEDIMIENTO ADMINISTRATIVO GENERAL, APROBADO POR DECRETO SUPREMO N° 004-2019-JUS**
Artículo 20.- Modalidades de notificación
(….)
20.4. El administrado interesado o afectado por el acto que hubiera consignado en su escrito alguna dirección electrónica que conste en el expediente puede ser notificado a través de ese medio siempre que haya dado su autorización expresa para ello. Para este caso no es de aplicación el orden de prelación dispuesto en el numeral 20.1.

La notificación dirigida a la dirección de correo electrónico señalada por el administrado se entiende válidamente efectuada cuando la entidad reciba la respuesta de recepción de la dirección electrónica señalada por el administrado. La notificación surte efectos el día que conste haber sido recibida, conforme lo previsto en el numeral 2 del artículo 25.

En caso de no recibirse respuesta automática de recepción en un plazo máximo de dos (2) días útiles contados desde el día siguiente de efectuado el acto de notificación vía correo electrónico, se procede a notificar por cédula conforme al inciso 20.1.1.

Lo señalado en el presente numeral no impide que la entidad asigne al administrado una casilla electrónica gestionada por ella, siempre que cuente con el consentimiento del administrado, salvo lo dispuesto en la tercera disposición complementaria final de la Ley Nº 30229 o norma que lo sustituya. En este caso, la notificación se entiende válidamente efectuada cuando la entidad la deposite en el buzón electrónico asignado al administrado, surtiendo efectos el día que conste haber sido recibida, conforme lo previsto en el numeral 2 del artículo 25.

Para la notificación por correo electrónico, la autoridad administrativa, si lo considera pertinente, puede emplear firmas y certificados digitales conforme a lo estipulado en la ley de la materia.

En ese sentido, determinadas con carácter preliminar las circunstancias que justifican la instauración del procedimiento sancionador, remitimos el presente informe y la Fiscalización N° 257-2020-DFI, que consta de quinientos sesenta y cuatro (564) folios para las acciones pertinentes.

Sin otro particular, es todo por cuanto tengo que informar.

PERÚ Ministerio de Justicia y Derechos Humanos
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Firmado digitalmente por VARGAS MARQUEZ Vanessa Antonella FAU 20131371617 soft
Fecha: 2021.05.03 22:21:52 -05'00'

.....

Vanessa Antonella Vargas Márquez
Analista Legal de Fiscalización
Dirección de Fiscalización e Instrucción.

OEV/vvm

BICENTENARIO PERÚ 2021