UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

2013

Resoluciones Dictámenes e Informes

JOSÉ ARTIGAS
UNIÓN DE LOS PUEBLOS LIBRES
BICENTENARIO.UY

agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

2013

Resoluciones Dictámenes e Informes

INDICE

RESOLUCIONES

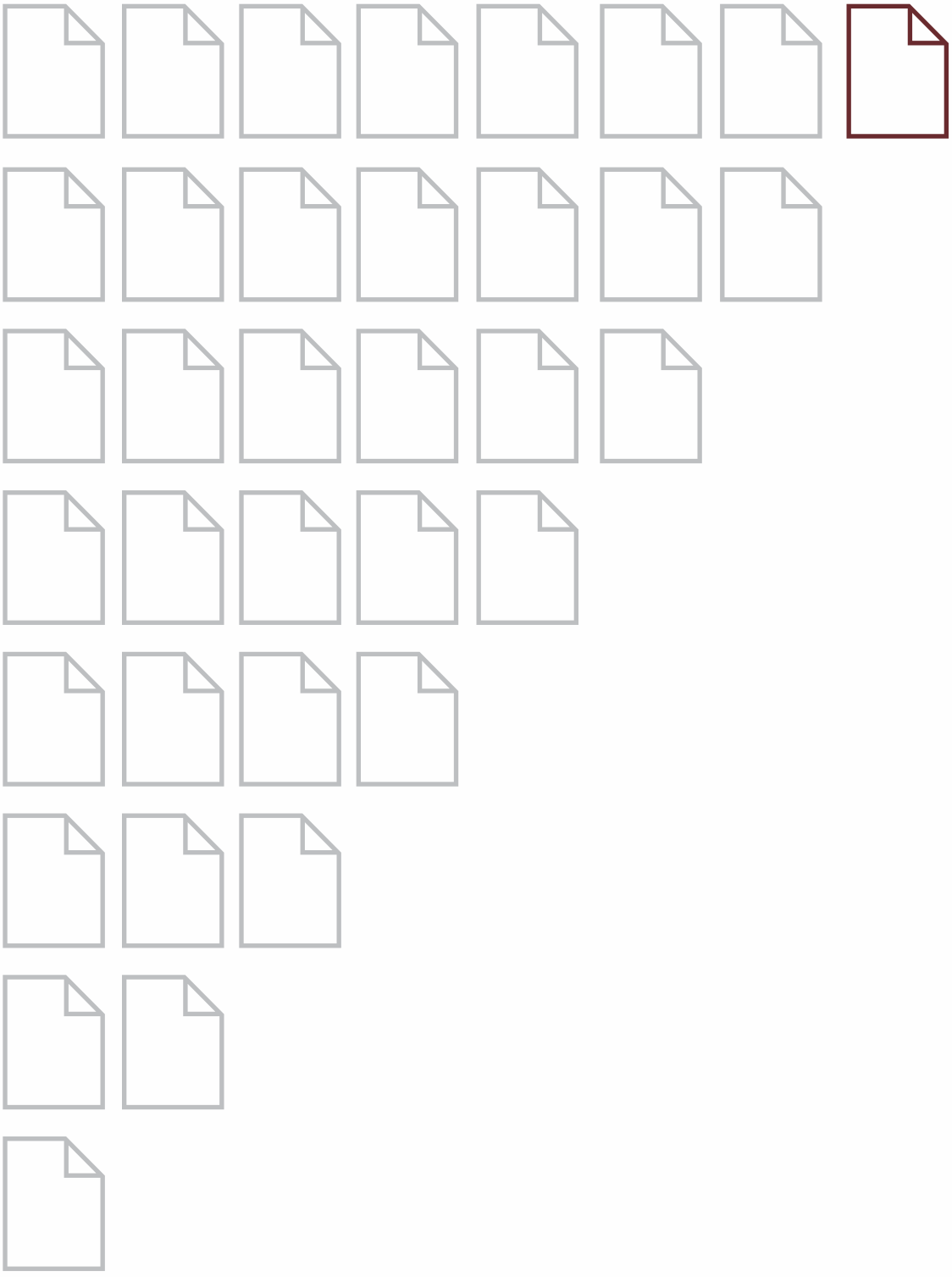
PAG.

DICTAMENES

PAG.

INFORMES

Resoluciones



Resolución Nº 5, de 21 de febrero de 2013.

Se resuelve denuncia sobre inclusión en base de datos de morosos.

RESOLUCION No.		EXPEDIENTE No.
5	2013	2012-2-10-0000168

Montevideo, 21 de febrero de 2013

VISTO:

La denuncia presentada contra AA.

RESULTANDO:

I) Que la denunciante alega haber sido acosada por esta empresa, al tratar de cobrarle una deuda que no le ha sido notificada y que ella desconoce.

II) Que es relevante indicar que se da vista a las empresas involucradas, las cuales presentan sus descargos y adjuntan documentación que acredita el contrato celebrado entre ambas para gestionar el cobro, así como los vales firmados por la denunciante. BB S.A también ha grabado las conversaciones mantenidas con la denunciante y las pone a consideración de la Unidad.

III) Que oportunamente se da vista a la denunciante pero no presenta más aclaraciones.

CONSIDERANDO:

I) Que se trata de una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 y su decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que no surge de la denuncia que la interesada haya ejercido el derecho de acceso (art. 14), sin embargo según su propio relato, ha sido advertida de la existencia de tal deuda en varias oportunidades a partir de diciembre del año 2011.

III) Que si bien BB S.A., le habría informado que no figuraba en su base de datos, ello se debería a que el art. 22 de la Ley determina que estos datos, pueden registrarse por un plazo de 5 años contados desde su incorporación, y en caso de vencimiento de dicho plazo, cuando la obligación se mantiene incumplida, el acreedor podrá solicitar un nuevo registro por otros 5 años.

IV) Que por otra parte, aunque dicha información ya no figura en esa base, en los descargos presentados por esta empresa se indica que, -según los datos proporcionados por su cliente (AA S.A.)-, efectivamente han procedido a gestionar el cobro de la deuda mediante un servicio que brindan a sus afiliados y se denomina AA.

V) Que en cuanto a los derechos de rectificación o de supresión (art.15), la denunciante no aporta la documentación necesaria para probar que, los datos que posee la empresa sobre su deuda con AA, es una información errónea o falsa.

VI) Que el art. 22 de la Ley, establece que queda expresamente autorizado el tratamiento

de datos personales destinados a brindar informes objetivos, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia, en aquellos casos en que los mismos sean procedentes de informaciones facilitadas por el acreedor.

VII) Que en definitiva, de la documentación aportada tanto por BB S.A. como por AA S.A., surge que la denunciante contrajo esas deudas y hasta la fecha no ha aportado prueba que permita inferir lo contrario.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Establecer el archivo sin perjuicio de estas actuaciones, pues el tratamiento se enmarca en lo establecido por la Ley para la información de carácter comercial o crediticia y responden a la realidad objetiva.
2. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 8, de 21 de febrero de 2013.

Se resuelve denuncia por instalación de cámaras de video vigilancia sin cumplir con el deber de de informar del artículo 13 de la Ley Nº 18.331.

RESOLUCION No.		EXPEDIENTE No.
8	2013	2011-2-10-0000644

Montevideo, 21 de febrero de 2013

VISTO:

La denuncia formulada ante la Unidad Reguladora y de Control de Datos personales por AA contra BB por la instalación de cámaras de vigilancia.

RESULTANDO:

I) Que AA presentó denuncia en virtud de la implementación en su lugar de trabajo de un sistema de reloj tarjetero que toma imágenes al momento de marcar las entradas y salidas del personal y las posibles implicancias que éste puede generar en el uso de su imagen y sus datos personales. Afirma que no se ha informado al personal acerca de la recolección de imágenes.

II) Que la denunciada alega que ha dado respuesta a la inquietud del denunciante y agrega, respecto a las imágenes de los funcionarios al momento de registrar su asistencia, que: "Dichas imágenes no pueden ser calificadas de manera alguna como datos personales, sino que se trata de un insumo que la Administración maneja -en uso de sus legítimas facultades-, a los efectos de ejercer su poder deber de supervisión". Indica además, que BB no ha realizado ningún acto que implique la vulneración de los datos del denunciante.

CONSIDERANDO:

I) Que la instalación de un sistema de registro de asistencia de funcionarios de la institución es una manifestación de su poder deber de supervisión respecto a éstos, pero ello no implica que las imágenes que se registren dejen por ello de ser datos personales que merecen protección.

II) Que frente a la instalación de las cámaras de seguridad, se ha debido informar a los funcionarios en forma previa ese hecho, y en el caso de que corresponda, identificar la existencia de éstas a través de los logos correspondientes.

III) Que se debió proceder a la inscripción de las bases de datos en las cuales se almacenan las imágenes a los efectos de dar cumplimiento al principio de legalidad establecido en la ley.

IV) Que corresponde tener en cuenta la primariedad de la infracción cometida.

ATENTO:

A lo preceptuado en los arts. 9º y 35 de la Ley N° 18.331, este último en su redacción dada por el art. 152 de la Ley N° 18.719 de 27 de Diciembre de 2010.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE

1. Sancionar con “observación” a BB por infracción a la Ley Nº 18.331 en virtud del tratamiento dado a los datos personales de sus funcionarios.
2. Establecer que la facultad de enfermería deberá instalar los logos de video vigilancia correspondiente y proceder a la inscripción de la base de datos en cumplimiento del principio de legalidad consagrado en la Ley Nº 18.331.
3. Notifíquese y publíquese.

Firmado:

Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución Nº 64, de 16 de mayo de 2013.

Se establece que todos los sitios web que realicen tratamientos de datos personales situados en el país deben publicar las condiciones relativas a este tratamiento.

RESOLUCION No.		Acta No.
64	2013	11

Montevideo, 16 de mayo de 2013

VISTO Y CONSIDERANDO:

I) Que es frecuente que los sitios web con datos personales de quienes acceden o se involucran a ellos.

II) Que en todos los casos se debe asegurar el cumplimiento del derecho a la protección de datos personales.

III) Que de acuerdo con la normativa vigente es preceptivo cumplir con los principios y deberes esenciales en la materia, en especial y entre otros lo relativo al "derecho de información" (art. 13 de la Ley Nº 18.331), y los principios de no excesividad o proporcionalidad, finalidad, consentimiento informado y (arts. 7º, 8º, 9º de la Ley).

ATENTO:

A lo precedentemente expuesto y a los artículos citados de la Ley Nº 18.331, sus modificativas y concordantes,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

Establecer que todo sitio web que efectúe tratamiento de datos personales en el Uruguay deberá publicar las condiciones relativas a dicho tratamiento, en adecuación a lo dispuesto por la Ley Nº 18.331.

Firmado:

Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Resolución Nº 66, de 23 de mayo de 2013.

Se resuelve denuncia por envío de correo electrónico no deseado.

RESOLUCION No.		EXPEDIENTE No.
66	2013	2012-2-10-0000534

Montevideo, 23 de mayo de 2013

VISTO:

La denuncia presentada por AA contra BB S.A., por envío de correo no deseado.

RESULTANDO:

I) Que la denunciante alega haber recibido spam, pero no aporta datos sobre el correo electrónico que los recepciona.

II) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a todas las partes.

III) Que la empresa denunciada manifiesta que cuentan con una base de datos de clientes de los vendedores. Asimismo, indica que la denunciante se niega a proporcionar su casilla de correo a fin de ser eliminada de la lista de envíos.

CONSIDERANDO:

I) Que estamos ante una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 y su decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que según lo indica la Ley es legítimo comunicarse por correo para ofrecer un producto, cuando se tiene conocimiento de ciertos datos personales que no requieren el consentimiento, cuando esos datos son aportados por los propios titulares o cuando figuran en documentos accesibles al público, pues tal actividad se enmarca en lo dispuesto por el art. 21 de la LPDP.

III) Que la empresa solicita que se aporte el correo para poder darlo de baja de su lista de envío de publicidad, pero sin embargo la denunciante no aporta tal información, ni se ha presentado ante la Unidad para indicar si ha ejercido el derecho de acceso (art. 14), ni a efectos de aportar nuevos elementos.

IV) Que debido a ello no surge de las actuaciones que el correo de la denunciante figure en una fuente accesible al público, así como tampoco se ha aportado por parte de la empresa, la prueba de que se ha recabado el consentimiento de la misma.

V) Que por su parte el art. 6° de la LPDP prevé que la formación de bases de datos será lícita cuando se encuentren debidamente inscriptas.

VI) Que en definitiva, corresponde considerar, que se ha incurrido por parte de la empresa, en un tratamiento que vulnera lo establecido en la LPDP, arts. 6° y 21 de la Ley.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con observación a BB S.A por infracción a la Ley Nº 18.331, arts. 6º y 21.

2. Intimar a inscribir las bases de datos, otorgando un plazo de 30 días a tales efectos, so pena de aplicar una sanción más severa.

3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Resolución Nº 91, de 17 de julio de 2013.

Se resuelve denuncia por colocación de cámaras de video vigilancia enfocadas hacia recintos particulares.

RESOLUCION No.		EXPEDIENTE No.
91	2013	2011-2-10-0000860

Montevideo, 17 de julio de 2013

VISTO:

La denuncia presentada por AA contra BB y CC, por video vigilancia dirigida hacia el fondo de su domicilio.

RESULTANDO:

I) Que la denunciante alega ser video vigilada por los denunciantes desde que ha procedido a denunciarlos por tener alrededor de 30 perros sin las condiciones apropiadas.

II) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a la parte denunciada en varias oportunidades pero ésta no se ha presentado a efectos de aportar las aclaraciones pertinentes.

III) Que asimismo se ha realizado inspección en el lugar constatando la existencia de cámaras de seguridad que apuntan hacia el fondo del domicilio de la denunciante, así como hacia la vereda ubicada frente al domicilio del denunciado.

CONSIDERANDO:

I) Que estamos ante una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 y su decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que la imagen es un dato personal cuyo tratamiento debe estar sujeto a la normativa de protección de datos personales, y salvo las excepciones previstas en la norma, el art. 9º establece que el tratamiento de datos es lícito cuando el titular hubiera prestado su consentimiento libre, expreso, previo, expreso e informado.

III) Que además, según lo indica la Ley en su art. 25 el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos.

IV) Que debido a ello, no surge de las actuaciones que exista un interés legítimo ni que el video vigilancia denunciada esté amparada por el marco legal, a lo que se suma que los denunciados no ha colaborado con la Unidad ni han aportado información que permita aclarar su situación.

V) Que en definitiva, corresponde considerar, que se incurre por parte de los denunciados

en un tratamiento que vulnera lo establecido en la LPDP, arts. 1°, 9°, 13 y 25.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con multa de 1.000 UI a BB y CC por infracción a la Ley Nº 18.331.

2. Realizar denuncia penal dado que las circunstancias emergentes de obrados tienen apariencia delictiva, a efectos de que los hechos sean investigados por la justicia.

3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 124, de 29 de agosto de 2013.

Se resuelve denuncia contra empresa financiera por el ofrecimiento de créditos pre – aprobados a través de llamadas telefónicas, incumpliendo disposiciones de la Ley Nº 18.331.

RESOLUCION No.		EXPEDIENTE No.
124	2013	2012-2-10-0000591

Montevideo, 29 de agosto de 2013

VISTO:

La denuncia presentada por AA, contra BB S.A. debido a que ha recibido varias llamadas de esta financiera, para ofrecerle un crédito ya pre aprobado, informándole que habrían obtenido sus datos de BB.

RESULTANDO:

I) Que la Unidad Reguladora y de Control de Datos Personales oportunamente realizó informes y confirió vista a la parte denunciada, habiéndose presentado ésta indicando que no posee base de datos y que no se le aplica la Ley N° 18.331. Tampoco ha aportado la información solicitada por la Unidad respecto a probar cómo ha obtenido el consentimiento de la denunciante

II) Que la URCDP asimismo ha realizado inspección a la sede constatando la existencia de base de datos y un sistema de video vigilancia en el local de la empresa en Juan Lacaze.

CONSIDERANDO: I) Que estamos ante una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 y su decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que sin embargo de la documentación que obra en el expediente no surge que los datos de la denunciante hayan sido obtenidos en forma fraudulenta o de forma que vulnere la Ley.

III) Que surge en cambio que BB SA solicita informes a CC cada vez que recibe solicitudes de crédito, de acuerdo con lo establecido en el art. 22 que autoriza el tratamiento de datos personales destinados a brindar informes objetivos, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia.

IV) Que sin embargo surge que BB S.A. no ha inscripto sus bases de datos, –cuya existencia fue verificada durante las dos inspecciones realizadas tanto a la sede de Juan Lacaze como donde se ubica su servidor en Montevideo-, no ha informado oportunamente a la denunciante en los términos indicados en el art. 13 de la Ley, ni ha aportado la documentación que acredite que efectivamente AA se presentó a solicitar el crédito.

V) Que al respecto corresponde tener presentes las facultades que le otorga la Ley a la URCDP (art. 34), en tanto Órgano de Control en la materia, que posee potestades legales inspectivas, así como la de solicitar información de antecedentes, documentos u otros

elementos relativos al tratamiento de datos personales por parte de entidades públicas y privadas.

VI) Que en definitiva, corresponde considerar, que se ha incurrido por parte del denunciado en un tratamiento que vulnera lo establecido en la LPDP, arts. 6º, 9º, 12 y 13.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Sancionar con apercibimiento a BB SA por infracción a los arts. 6º, 9º, 12 y 13 de la Ley Nº 18.331.

2. Otorgar un plazo de treinta (30) días a efectos de que se presente a inscribir sus bases de datos, so pena de aumentar la sanción a imponer.

3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 137, de 12 de setiembre de 2013.

Se resuelve denuncia por comunicación ilícita de datos personales.

RESOLUCION No.		EXPEDIENTE No.
137	2013	2011-2-10-0000637

Montevideo, 12 de setiembre de 2013

VISTO:

La denuncia presentada por AA contra BB S.A. (en adelante BB).

RESULTANDO:

I) Que la denunciante alega que sus datos fueron aportados por un tercero con el fin de afiliarla a la Institución Mutual, y posteriormente transmitidos a CC S.A. a efectos de que se gestionara la deuda por falta de pago.

II) Que la Unidad Reguladora y de Control de Datos Personales oportunamente confirió vista a las partes.

CONSIDERANDO: I) Que se está ante una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 y su decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que la denunciante relata que no conoce a la persona que la afilió a BB e indica no haber generado adeudo alguno con esta empresa, y efectúa otras consideraciones al respecto.

III) Que la documentación contractual agregada del folio Nº 29 al 32 de por sí irregular bajo la óptica de derecho común (se trata de un pliego de 4 folios firmado por única vez al pie del primero y no al final como marca la ley) no está suscrita ni autorizada por la denunciante, creándole una situación jurídica gravosa sin su consentimiento.

IV) Que por lo tanto, el tratamiento de los datos personales por parte de BB adoleció de una muy señalada ilicitud.

V) Que además, si bien la queja presentada por la damnificada dio como resultado la eliminación de los datos, ello se hizo fuera de los plazos legales establecidos por el art. 15 de la Ley Nº 18.331.

VI) Que corresponde considerar a su vez que CC S.A. es un encargado de tratamiento porque sus funciones en este caso, encuadran en el art. 4° lit. H), que determina que el encargado de tratamiento es toda persona física o jurídica, pública o privada, que sola o en conjunto con otros, trate datos personales por cuenta del responsable de la base de datos o del tratamiento. En este caso el responsable de la base de los clientes es BB.

VII) Que es pertinente señalar además como un agravante, que BB no tenía sus bases de datos debidamente inscriptas a la fecha en que han sucedido los hechos.

VIII) Que en definitiva, corresponde considerar, que se ha incurrido por parte de la UCM en un tratamiento que vulnera lo establecido en la LPDP, arts. 6º, 7º, 9º, 10, 12, 13,14 y 15.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE

1. Aplicar una sanción de 12.001 U.I. a BB por infracción a la Ley Nº 18.331.
2. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Resolución Nº 181, de 19 de diciembre de 2013.

Se resuelve denuncia relativa a la solicitud de daos personales en las ventas a crédito.

RESOLUCION No		EXPEDIENTE No
181	2013	2012-2-100000891

Montevideo, 19 de diciembre de 2013

VISTO:

La denuncia presentada por AA contra BB y CC S.A, ante la solicitud de ciertos datos personales al momento de abonar con cheque obsequio o con tarjeta de crédito.

RESULTANDO:

I) Que la Unidad otorga vista por el término de diez días hábiles a BB, las que fueran evacuadas en tiempo y forma.

II) Que BB S.A. manifiesta que se solicitan esos datos únicamente en las ventas a crédito y en cuanto a los cheques obsequio, se trata de promociones organizadas por DD S.A. (DD), dónde a texto expreso se establece que no será obligatoria su aceptación por parte de los comercios.

III) Que la denunciante reitera que no está dispuesta a brindar otros datos para utilizar el cheque obsequio, pues al hacer la compra en los locales adheridos a la promoción “Sonrisas”, éste debe ser aceptado sin necesidad de recabar otros datos.

IV) Que para un mejor diligenciamiento se solicita a EE y a DD S.A., que agreguen los términos contractuales de “Sonrisas”, así como la lista de locales adheridos y un modelo de cheque obsequio, los cuales se presentan y adjuntan.

CONSIDERANDO:

I) Que se está ante una situación alcanzada por la Ley N° 18.331 de 11 de agosto de 2008 y su Decreto reglamentario N° 414/009 de 31 de agosto de 2009.

II) Que no obstante ello, más allá de las relaciones comerciales acordadas entre dichas empresas en beneficio de sus clientes, estrictamente desde el punto de vista de los cometidos y potestades otorgados por la Ley N° 18.331 a la URCDP, no se identifica un tratamiento desproporcionado de los datos, que habilite considerar que se han vulnerados los principios de la norma, sobre todo los de consentimiento, finalidad y proporcionalidad.

III) Que sin embargo, se estima del caso que estas empresas deben adaptar el contenido de sus contratos a las obligaciones impuestas por la Ley, a efectos de recolectar sólo los datos necesarios e imprescindibles para realizar sus transacciones, así como deben informar a todos sus clientes en los términos previstos en el art. 13 de la Ley, con la finalidad de evitar conflictos más graves en el futuro que habiliten la aplicación de sanciones.

IV) Que en definitiva, una vez realizadas dichas recomendaciones, desde el punto

de vista de la protección de datos personales, corresponde el archivo sin perjuicio de las actuaciones.

ATENTO:

A lo expuesto y a lo previsto en las normas legales citadas

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES RESUELVE:

1. Recomendar a BB y a CC S.A, adaptar el contenido de sus contratos a las obligaciones impuestas por la Ley N° 18.331, recolectar los datos necesarios e imprescindibles para realizar las transacciones, así como informar a sus clientes en los términos previstos en el art. 13.

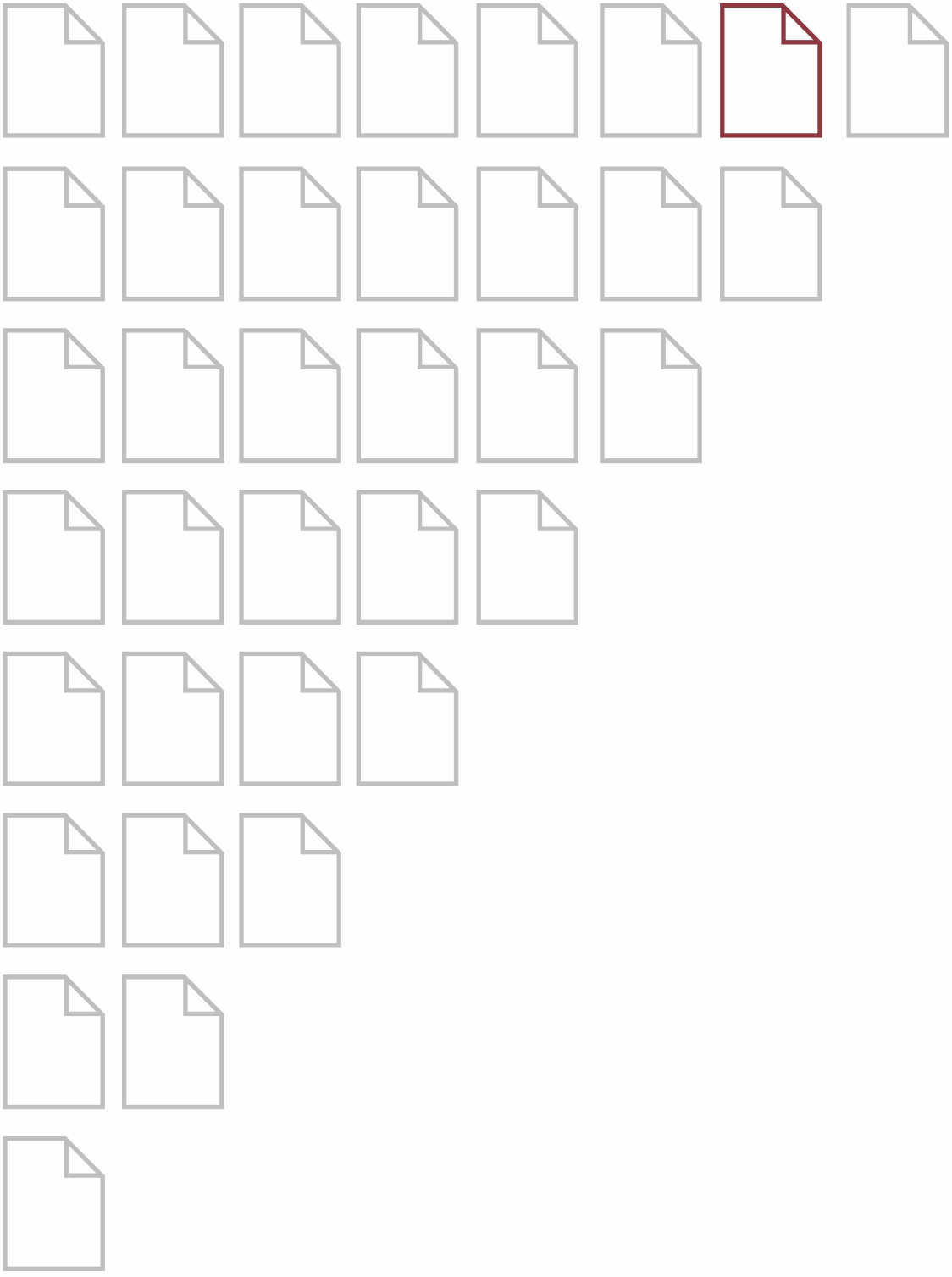
2. Establecer que corresponde el archivo sin perjuicio de estas actuaciones, previo conocimiento por parte de las empresas de las recomendaciones realizadas.

3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictámenes



Dictamen Nº 1, de 21 de febrero de 2013.

Se dictamina sobre la consulta de la Unidad de Acceso a la Información Pública (UAIP) relativa a si la Dirección Nacional de Medio Ambiente (DI. NA.MA.) está habilitada para comunicar a terceros información que recibe de empresas.

DICTAMEN No.		EXP. No.
1	2013	2012-2-10-0000649

Montevideo, 21 de febrero de 2013

VISTO:

La opinión solicitada por la Unidad de Acceso a la Información Pública – U.A.I.P. con relación a la consulta que formulara la Dirección Nacional de Medio Ambiente – DI.NA.MA.

RESULTANDO:

I) Que el planteo de la DI.NA.MA. alude a si está habilitada legalmente para comunicar a terceros que lo solicitan, cierta información que recibe de empresas.

II) Que en concreto se trata de Índices Ambientales de Operación (IAO), volúmenes de agua utilizada y su fuente, y efluentes.

III) Que ante el planteo recibido, la U.A.I.P. se dirige a nuestra Unidad a efectos que se pronuncie sobre si dicha información puede considerarse “confidencial”, y quedar por ello cubierta por el numeral II del art. 10 de la Ley Nº 18.381.

CONSIDERANDO:

I) Que el tipo de información a que alude la DI.NA.MA. en su consulta ingresa en la categoría de “dato personal”, en la medida que constituyen rasgos o cualidades con suficiente fuerza como para favorecer la determinabilidad a sus titulares.

II) Que el principio del previo consentimiento informado constituye uno de los pilares y garantías esenciales del derecho a la protección de datos personales, sin perjuicio de las excepciones que la Ley Nº 18.331 habilita para su no exigencia en ciertas hipótesis concretas.

III) Que en caso de acuerdos de intercambio de información entre entidades públicas es de regla, también, la vigencia del mismo principio, como lo tiene consignado la ley en la materia.

ATENTO:

A lo precedentemente expuesto, a lo dispuesto por los arts. 4º lit. D), 9º y 17 de la Ley Nº 18.331 de 11 de agosto de 2008, al art. 10 nal. II de la Ley Nº 18.381 de 17 de octubre de 2008, los arts. 157 y 158 lit. D) de la Ley Nº 18.719 de 27 de Diciembre de 2010, y el Informe Letrado Nº 12/2013

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Que la información mencionada en la consulta elevada por la DI.NA.MA. a la U.A.I.P. tiene naturaleza de “datos personales”.

2. Que en consecuencia, salvo consentimiento del titular o aplicación de alguna de las excepciones previstas en los arts. 9º y 17 de la Ley Nº 18.331, dicha información ingresa en la categoría de “información confidencial” en aplicación del art. 10 nal. II de la Ley Nº 18.381.

3. Que procede devolver las actuaciones a la U.A.I.P. con el presente dictamen pronunciado a su solicitud.

Firmado:

Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen Nº 2, de 21 de febrero de 2013.

Se dictamina sobre la consulta de la Dirección Nacional de Sanidad Policial del Ministerio del Interior sobre la instalación de cámaras de video vigilancia en diversas áreas del Hospital Policial.

DICTAMEN No.		Expediente No.
2	2013	2012-2-10-0000866

Montevideo, 21 de febrero de 2013

VISTO:

La consulta presentada por el Ministerio del Interior-Dirección Nacional de Sanidad Policial sobre la instalación de cámaras de video vigilancia en diversas áreas del Hospital Policial.

RESULTANDO:

I) Que la consulta se origina en una solicitud de compra de cámaras con circuito cerrado de televisión para el Área de Cuidados Críticos del Hospital Policial con el objetivo de lograr una vigilancia más estrecha, permitiendo mayor seguridad para los pacientes y para el personal que allí se desempeña.

II) Que el expediente pasó a informe jurídico, el cual se realizó con fecha 27 de noviembre de 2012.

CONSIDERANDO:

I) Que la Unidad se ha expedido en el Dictamen N° 76 de 2009 determinando que la captación o grabación de imágenes constituye información personal, por lo que resulta de aplicación la normativa vigente sobre la protección de datos, teniendo en cuenta los diversos aspectos comprendidos, lo que puede ser video vigilado, de qué forma, qué principios son aplicables, si se deben registrar los resultados de la video vigilancia, y las situaciones en que la normativa no resulta aplicable.

II) Que la video vigilancia debe utilizarse en forma proporcional a la finalidad, o sea cuando no existan otros medios menos lesivos a la privacidad que permitan obtener los mismos resultados, y atendiendo a los principios de protección de datos personales consagrados en la normativa.

ATENTO:

A lo establecido en la LPDP y a lo precedentemente expuesto,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Establecer que la video vigilancia debe utilizarse en forma proporcional a la finalidad y cuando no existan otros medios menos lesivos a la privacidad que permitan obtener los mismos resultados, y se deberán atender a los principios consagrados en la Ley N° 18.331 prestando especial atención a los principios de legalidad, consentimiento informado y finalidad

2. Recomendar la colocación de los logos de video vigilancia con la identificación del responsable, y si correspondiere, inscribir la o las bases de datos.

3. Notifíquese, y oportunamente publíquese.

Firmado:

Dr. Felipe Rotondo

Consejo Ejecutivo URCDP

Dictamen Nº 3, de 4 de marzo de 2013.

Se dictamina sobre la consulta del Ministerio de Salud Pública respecto a la posibilidad de entregar certificados de defunción a las compañías aseguradoras.

DICTAMEN No.		Expediente No.
3	2013	2012-2-10-0000893

Montevideo, 4 de marzo de 2013

VISTO:

La consulta presentada por el Ministerio de Salud Pública respecto a la entrega de certificados de defunción a compañías aseguradoras.

RESULTANDO:

I) Que la consulta se presenta en virtud de un recurso de revocación y jerárquico presentado ante el consultante por parte de una empresa aseguradora, contra un acto administrativo en el cual se establecen una serie de requisitos para la entrega de certificados de defunción, que le causa perjuicios.

II) Que el expediente pasó a informe jurídico, el cual se realizó con fecha 27 de noviembre de 2012.

CONSIDERANDO:

I) Que el certificado de defunción es un documento que contiene datos personales de naturaleza sensible, los cuales se encuentran especialmente protegidos por la Ley Nº 18.331.

II) Que el contrato de seguro de vida es de carácter voluntario prestando el tomador o suscriptor su consentimiento en forma libre, expresa y escrita. Se trata de un contrato cuya ejecución tendrá lugar una vez fallecido el suscriptor, y ésta depende en varios casos de factores relacionados a la causal de su muerte que no lucen en la partida de defunción.

III) Que lo informado refiere específicamente a la normativa de protección de datos personales y debe tratarse conjuntamente con las normas específicas en la materia.

ATENTO:

A lo establecido en la LPDP y a lo precedentemente expuesto,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Establecer que de acuerdo a la normativa analizada es posible entregar la información en cuestión, teniendo en cuenta que deben armonizarse la Ley Nº 18.331, con las normas relativas a derechos y deberes de los usuarios de la salud, y las demás normas y disposiciones específicas en la materia que la complementan.

2. Recomendar atender a los principios generales de la protección de datos personales

a los efectos de resolver situaciones dudosas.

3. Notifíquese, y oportunamente publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 4, de 4 de marzo de 2013.

Se dictamina respecto a la consulta formulada por el Edil Fernando Riet referente a si de acuerdo con lo dispuesto en el artículo 16 de la Ley Nº 9.515, cualquier Edil puede pedir al Intendente datos e informes que sean necesarios para cumplir con sus cometidos, y qué datos personales de de los funcionarios no se pueden enviar.

DICTAMEN No.		EXPEDIENTE No.
4	2013	2012-6-1-0000953

Montevideo, 4 de marzo de 2013

VISTO:

La consulta formulada por el Edil Fernando Riet.

RESULTANDO:

Que la misma refiere a si de acuerdo al art.16 de la Ley Nº 9.515, todo Edil puede pedir al Intendente los datos e informes que estime necesarios para llenar su cometido y si existiendo base de datos de los funcionarios de la Intendencia registrada de acuerdo a normas de la Ley de Habeas Data, ¿qué datos no se deben enviar de los funcionarios?

CONSIDERANDO:

I) Que si bien es cierto que el pedido de informes realizado por un Edil Departamental se enmarca en lo establecido en la Ley N° 9.515 y en lo previsto en el art. 284 de la Constitución, corresponde tener presente también, que la Ley N° 18.331 consagra un derecho humano y un sistema de protección especial que emana de la propia Carta Magna, así como del Derecho Internacional de los Derechos Humanos.

II) Que por ello es necesario equilibrar los derechos e intereses en juego a la luz de los diferentes principios que guían la protección de datos personales, sobre todo los de consentimiento, finalidad y proporcionalidad (arts. 5° y 8°), así como en cada caso debe existir un juicio de proporcionalidad basado en la idoneidad, la necesidad de los datos y el equilibrio de derechos, que deberá ser especialmente riguroso cuando esté presente información personal especialmente sensible como son, entre otros, los datos de ideología, afiliación sindical, creencias religiosas, origen étnico, salud o vida sexual.

III) Que hay datos personales de los funcionarios públicos que deben considerarse públicos pues emanan de la naturaleza misma de la función que cumplen (art.38 del Decreto N° 232, reglamentario de la Ley N° 18.381), así como hay otros que de acuerdo al art. 9° lit. C) de la Ley N° 18.331, no requieren el previo consentimiento informado para su tratamiento.

IV) Que en definitiva, el problema se debe plantear respecto a aquellos datos que requieren para su comunicación o cesión el previo consentimiento informado de su titular y/o se trata de datos de carácter sensible, para lo cual deberá realizarse la ponderación adecuada

caso a caso, cuando se solicita acceder a determinada información en poder del sector público en aras de la transparencia y la rendición de cuentas, prueba que se conoce como Prueba de Interés Público en el derecho comparado.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que desde el punto de vista de la protección de datos personales, las Intendencias sólo estarán legitimadas para entregar al solicitante los datos personales de los funcionarios relacionados con el cargo y las funciones que ocupan, así como los datos que el art. 9° lit. C) de la Ley N° 18.331 enumera taxativamente y que no requieren el previo consentimiento informado para su tratamiento.

2. Notifíquese, publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 5, de 14 de marzo de 2013.

Se dictamina sobre la consulta formulada por el Banco de Previsión Social (BPS), el Ministerio de Educación y Cultura (MEC) y las Asociaciones que vinculan Instituciones de Enseñanza Privada respecto a si pueden solicitarle a éstas ultimas, información sobre escolares y liceales para facilitar el otorgamiento y control del beneficio de la Asignación Familiar.

DICTAMEN No.		EXPEDIENTE. No.
5	2013	2013-2-10-000096

Montevideo, 14 de marzo de 2013

VISTO:

La consulta conjunta formulada por el Banco de Previsión Social (BPS), el Ministerio de Educación y Cultura (MEC) y las Asociaciones que vinculan a las Instituciones de Enseñanza Privada (EIHU-IAHU y AUDEC), respecto a si resulta acorde al régimen de protección de datos personales solicitarle a las Instituciones de Enseñanza Privada los datos de escolares y liceales que se especifican en la consulta, con la finalidad de facilitar el otorgamiento y control del beneficio de Asignación Familiar que sirve el Ente.

RESULTANDO:

I) Que el planteo se basa en razones de buena administración, en la medida que, como se sostiene, la comunicación redundará en beneficio de los propios beneficiarios y se cumplirá real y efectivamente la legislación vinculada a dicha prestación, al tiempo de evitar tener que citar a cada interesado para volver a requerirle una información que ya está disponible.

II) Que los datos cuya comunicación se pretende son: cédula de identidad, nombre completo, fecha de nacimiento, fecha de matriculación, indicador de permanencia en los estudios (o asistencia regular, o progreso educativo) que justifica ser acreedor de la prestación, indicador de recibo o postulación a recibir el beneficio.

CONSIDERANDO:

I) Que la comunicación en los términos planteados, se enmarca en los principios que rigen la materia de protección de datos personales, en particular los de legalidad, veracidad (por lo que refiere a su adecuación, ecuanimidad y no excesividad), y finalidad.

II) Que de acuerdo con el régimen legal vigente no resulta necesario contar con el consentimiento de los titulares de los datos (o de sus representantes legales en el caso), para comunicaciones del orden de las que plantea la consulta, circunscripta a datos de personas y grupos familiares atributarios del régimen de Asignación Familiar, no así a todos los alumnos.

ATENTO:

A lo precedentemente expuesto, al Informe Letrado que antecede, y a lo dispuesto por los arts.

6º, 7º, 8º y 9º lits. B) y C), y 17 lit. B) de la Ley 18.331 y sus modificativas, así como en las Leyes Nº. 15.084 y Nº 18.227.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

Se considera lícita la comunicación de datos personales que plantea la consulta, en poder de las Instituciones de Enseñanza Privada al Banco de Previsión Social, no requiriendo el consentimiento de los titulares respecto, específicamente, a personas y grupos familiares que son atributarios o gestionantes del beneficio de Asignación Familiar, a los efectos de facilitar y controlar el otorgamiento y mantenimiento de éste; para otros casos, se tendrá por lícita la comunicación solamente con consentimiento del titular de los datos, o sus representantes legales, en los términos que prevé la Ley Nº 18.331.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 6, de 21 de marzo de 2013.

Se dictamina sobre la consulta de la Unidad de Información Nacional de Salud (UINS) sobre la inclusión en la nueva versión del certificado de defunción, impreso y electrónico, del número de teléfono celular y del correo electrónico del médico certificador.

RESOLUCION No.		EXPEDIENTE No
6	2013	2013-2-10-0000080

Montevideo, 21 de marzo de 2013

VISTO:

La consulta realizada por la Unidad de Información Nacional de Salud (UINS), sobre la pertinencia de incluir en la nueva versión del Certificado de Defunción impreso y electrónico, el número de teléfono celular y/o correo electrónico del médico certificador.

CONSIDERANDO:

I) Que según Informe N° 49 de 12 de Marzo de 2013, la inclusión en el Certificado de Defunción de los datos teléfono fijo o celular, y correo electrónico del médico certificador, no contraría las disposiciones de la Ley N° 18.331.

II) Que se trata de una comunicación de datos excepcionada del requisito del previo consentimiento informado de su titular, conforme lo dispuesto en los lits. B) y D) del art. 9º de la citada norma, siendo el interés legítimo el cuidado de la Salud en cuanto bien supremo.

III) Que de acuerdo con la normativa nacional vigente, el Certificado de Defunción forma parte de la Historia Clínica, y su llenado completo e inteligible por parte del médico certificador es una obligación que debe ser cumplida.

ATENTO:

A lo expuesto, y a lo dispuesto por los arts. 31 y 34 de la Ley N° 18.331,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que la inclusión en el Certificado de Defunción de los datos teléfono fijo o celular, y correo electrónico del médico certificador, no contraría las disposiciones de la Ley N° 18.331.

2. Señalar que se trata de una comunicación de datos exceptuada del requisito del previo consentimiento informado de su titular.

3. Resaltar que el Certificado de Defunción forma parte de la Historia Clínica, y su llenado completo e inteligible por parte del médico certificador es obligatoria.

4. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 8, de 21 de marzo de 2013.

Se dictamina sobre la consulta de la Dirección General de Registro de Estado Civil sobre el alcance de la Ley Nº 18.331 respecto a la información contenida en el acta y certificado de defunción del Mtro. Julio Castro.

DICTAMEN No.		EXPEDIENTE No.
8	2013	2013-2-10-0000051

Montevideo, 21 de marzo de 2013

VISTO:

La consulta formulada por la Dirección General de Registro de Estado Civil referida al alcance que posee la Ley N° 18.331 respecto a la información contenida en Acta y Certificado de Defunción del Mtro. Julio Castro.

RESULTANDO:

I) Que a pedido expreso de un familiar se incluye en el Acta de Defunción la causa de su muerte que ha sido determinada por el Equipo de Médicos Forenses, como resultado del "disparo de arma de fuego en contexto de tortura y malos tratos".

II) Que sin embargo, la Dirección General del Registro de Estado Civil dictó una circular (Circular N° 2/2012 de 2 de marzo de 2012), en la que se establece que al labrar el acta de defunción, ya sea en certificado electrónico o en papel, no deberá dejarse constancia de la causa de la muerte si en el certificado no viene establecida. En caso de que se haya indicado, deberá dejarse constancia de que es reservada de acuerdo a la normativa de datos personales.

CONSIDERANDO:

I) Que corresponde analizar los fundamentos legales de dicha reserva establecida en el Decreto del Poder Ejecutivo de 8 de diciembre de 2011 sobre Certificado de Defunción Electrónica, recogidos en la Circular N° 2/2012 de la Dirección General de Registro de Rstado Civil, Ley N° 18.335 sobre Derechos de los Pacientes y Usuarios y su Decreto N° 274/010 y Ley N° 18.331 de Protección de Datos y Acción de Habeas Data.

II) Que de la Ley N° 18.335 y su Decreto, no surge en forma expresa que la causa de la muerte deba ser considerada, por sí sola, un dato clínico reservado, sino que esas normas refieren al tratamiento de la información que consta en la historia clínica (propiedad del paciente), considerando que es reservada y que debe ser tratada de acuerdo a lo previsto en su art. 18. Además según lo indica el art. 1°, regula los derechos y obligaciones de los pacientes y usuarios de los servicios de salud, con respecto a los trabajadores de la salud y a los servicios de atención de la salud, en virtud de ello no corresponde su aplicación al caso que se consulta.

III) Que respecto a la Ley N° 18.331, cabe considerar que si bien se establece la reserva como uno de sus principios, también hay excepciones que deben ser debidamente armonizadas con los demás derechos que se contraponen en cada caso concreto.

IV) Que el art. 17 establece que los datos personales objeto de tratamiento podrán ser comunicados sin previo consentimiento cuando así lo disponga una ley de interés general, por ello en este caso, deberían considerarse especialmente tanto la Ley N° 18.381 de Acceso a la Información Pública (arts. 9, 10 y 12), como la Ley N° 18.596 de actuación ilegítima del Estado entre el 13 de junio de 1968 y el 28 de febrero de 1985 y Reconocimiento y Reparación a las Víctimas, además de la normativa de derecho internacional de los DD.HH. que nuestro país ha ratificado y que garantiza derechos a las víctimas de terrorismo de Estado.

V) Que el art. 17 a su vez señala, que no será necesario el consentimiento, cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. En el caso del Mtro. Julio Castro, la causa de la muerte es un dato que ha sido publicado en diversos medios de información, así como ya es parte de libros o informes oficiales que tienen circulación pública y masiva.

VI) Que para finalizar, corresponde la aplicación de la modificación introducida al art. 9 de la Ley N° 18.331, por el art. 43 de la Ley N° 18.996 de 7 de noviembre de 2012, estableciendo que se consideran como fuentes públicas o accesibles al público, entre otras, a las publicaciones oficiales y las publicaciones en medios masivos de comunicación, en cualquier soporte, así como a todo registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos, puedan ser consultados, difundidos o utilizados por parte de terceros.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que desde el punto de vista de la protección de datos personales, la Dirección General de Registro de Estado Civil se encuentra habilitada para incluir la causa de la muerte en el Acta y en la Partida de Defunción del Mtro. Julio Castro.

2. Notifíquese, publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 9, de 21 de marzo de 2013.

Se dictamina sobre la consulta del Ministerio de Educación y Cultura por un pedido de acceso a la información pública que recibe, en el cual se le solicita acceder al domicilio y al teléfono del titular de dicha Institución.

DICTAMEN No.		EXPEDIENTE No.
9	2013	2013-11-0001-0602

Montevideo, 21 de marzo de 2013

VISTO:

La consulta formulada por el Ministerio de Educación y Cultura en virtud de que recibe una solicitud de acceso a la información pública en el marco de la Ley N° 18.381, mediante la cual se solicita acceder al domicilio y al teléfono particular del titular de dicha institución.

RESULTANDO:

I) Que corresponde realizar la ponderación de los derechos e intereses en juego (en el caso acceso a la Información pública y protección de datos personales), a la luz de los diferentes principios que guían o estructuran la Ley N° 18.331, sobre todo los de consentimiento, finalidad y proporcionalidad.

II) Que se debe realizar un juicio de proporcionalidad que muestre como imprescindible la utilización de esa información, por ejemplo para investigar un delito, para mejorar la transparencia de la administración, evitar un peligro inminente o contribuir a una investigación judicial o administrativa.

CONSIDERANDO:

I) Que el art. 7° de la Ley N° 18.331 contempla la necesidad de que el tratamiento y/o comunicación de un determinado dato personal, deba ser proporcional a la finalidad que lo motiva y el art. 8° a su vez, establece que los datos objeto de tratamiento no podrán utilizarse para finalidades distintas, o incompatibles a aquellas que motivaron su obtención.

II) Que la finalidad implícita en una solicitud de acceso a la información pública, -prevista en la Ley N° 18.381-, es ejercer el control sobre la gestión y el funcionamiento de la administración, pero para alcanzar algunos de estos fines, no sería necesario pero sí desproporcionado, brindar acceso a información personal del Ministro, pues ella no alude al cargo y función que cumple, tal como se establece en el art. 38.8 del Decreto N° 232/010 reglamentario de la Ley N° 18.381.

III) Que no es de aplicación al caso lo establecido en el art. 9° B) de la Ley N° 18.331, que establece que no será necesario el previo consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, pues esta situación abarca a la recolección de datos por parte de un organismo, a efectos de poder cumplir con sus funciones, o cuando esta recolección se encuentra habilitada

por una ley.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que no es proporcional ni se ajusta al principio de finalidad brindar acceso al domicilio y teléfono personal del Ministro.

2. Notifíquese, publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 11, de 11 de abril de 2013.

Se dictamina sobre la consulta del Colegio de Contadores, Economistas y Administradores del Uruguay respecto a si es posible que la Caja de Jubilaciones y Pensiones Profesionales Universitarias facilite a una empresa encuestadores los teléfonos de los integrantes de la muestra aleatoria que no sean socios del Colegio de Contadores.

DICTAMEN No.		EXPEDIENTE No.
11	2013	2012-6-10-0000045

Montevideo, 11 de abril de 2013

VISTO:

La consulta formulada por el Colegio de Contadores, Economistas y Administradores del Uruguay sobre si es posible que la Caja de Jubilaciones y Pensiones de Profesionales Universitarios facilite a la empresa encuestadora los teléfonos de aquellos integrantes de la muestra aleatoria que no sean socios del Colegio de Contadores.

CONSIDERANDO:

I) Que en el caso no será posible omitir la solicitud del consentimiento, dado que no se trata de un dato amparado en las excepciones del art. 9º lit. C) de la Ley Nº 18.331.

II) Que se trata de una comunicación de datos personales, específicamente de datos telefónicos, de la Caja de Jubilaciones y Pensiones de Profesionales Universitarios a la empresa encuestadora.

III) Que para que esa comunicación de datos sea legítima conforme la citada Ley, deben cumplirse los requisitos contemplados en el art.17, que refieren con carácter general, al cumplimiento de los fines directamente relacionados con los intereses legítimos del emisor y destinatario, siempre que se cuente con el consentimiento de los titulares de los datos.

ATENTO:

A lo dispuesto en las normas citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. La Caja de Jubilaciones y Pensiones de Profesionales Universitarios deberá obtener el consentimiento de los Profesionales Universitarios, previo a facilitar a la empresa encuestadora los teléfonos de aquellos integrantes de la muestra aleatoria, sean o no socios del Colegio de Contadores.

2. Notifíquese, publíquese

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 12, de 18 de abril de 2013.

Se dictamina sobre la implementación de un área video vigilada y el procedimiento adecuado para la instalación de las cámaras.

DICTAMEN No.		EXPEDIENTE No.
12	2013	2012-2-10-0000942

Montevideo, 18 de abril de 2013

VISTO:

La consulta formulada por Osvaldo Enrique Cardozo y José Carlos Tavares, integrantes de la Comisión Administradora del Edificio Poseidón en sus calidades de Presidente y Secretario respectivamente, en relación a: 1) la obtención del consentimiento de la copropiedad del Edificio Poseidón respecto a la implementación de un área video vigilada resuelto por mayoría simple en Asamblea de Copropietarios y, 2) respecto al procedimiento adecuado para la implementación e instalación de cámaras que se implementará en el Edificio Poseidón, a efectos de dar cumplimiento a la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data y su decreto reglamentario.

RESULTANDO:

I) Que debido a acontecimientos relacionados con la seguridad del Edificio, la Comisión Administradora implementó un área video vigilada en el mismo. Se instalaron tres cámaras: dos en el palier de entrada al Edificio y la tercera en el salón común.

II) Que con fecha 25 de setiembre de 2012, se tomó conocimiento de una citación a audiencia por una demanda entablada por 29 vecinos que se encontraban disconformes con la implementación del sistema de video vigilancia por haberse resuelto sin haber convocado a una asamblea previa para deliberar sobre el tema.

III) Que en sede judicial se homologó un acuerdo en el cual la parte demandada se compromete a retirar las cámaras y se acuerda fijar una asamblea de copropietarios en un plazo máximo de 30 días a efectos de resolver sobre la instalación de cámaras en el edificio.

IV) Que realizada la asamblea, se resolvió por mayoría simple de presentes la instalación de las cámaras de video vigilancia con la finalidad de mejorar la seguridad del edificio.

V) Que existen copropietarios que no están de acuerdo con la instalación de dichas cámaras argumentando que la decisión tomada en la Asamblea de Copropietarios, debería ser por unanimidad de votos.

VI) Que en este marco, se consulta sobre 1) la obtención del consentimiento de la copropiedad del Edificio Poseidón respecto a la implementación de un área video vigilada resuelto por mayoría simple en Asamblea de Copropietarios y, 2) respecto al procedimiento adecuado para la implementación e instalación de cámaras que se implementará en el Edificio Poseidón, a efectos de dar cumplimiento a la Ley N° 18.331 de Protección de Datos Personales

y Acción de Habeas Data y su decreto reglamentario.

CONSIDERANDO:

I) Que respecto a la obtención del consentimiento de la copropiedad del Edificio referente a la implementación de un área video vigilada, se entiende que no es competencia de la Unidad expedirse en materia de régimen de Propiedad Horizontal, lo cual deberá resolverse por la vía correspondiente.

II) Que respecto al procedimiento adecuado para la implementación e instalación de cámaras que se implementará en el Edificio Poseidón, se deberá dar cumplimiento a la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data y sus normas complementarias, vale decir al régimen jurídico conocido bajo el nombre “derecho a la protección de datos personales”, debiéndose proceder de acuerdo al Dictamen 10/010, de 16 de abril de 2010, de la Unidad.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Respecto a la obtención del consentimiento de la copropiedad del Edificio referente a la implementación de un área video vigilada, se entiende que no es competencia de la Unidad expedirse en materia de régimen de Propiedad Horizontal, lo cual deberá resolverse por la vía correspondiente.

2. Respecto al procedimiento adecuado para la implementación e instalación de cámaras que se implementará en el Edificio Poseidón, se deberá proceder conforme al Dictamen de la Unidad N° 10/010, de 16 de abril de 2010.

3. Notifíquese, publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 14, de 16 de mayo de 2013.

Se dictamina sobre la consulta formulada por el Ministerio de Relaciones Exteriores relativa a la adecuación de un proyecto de Convenio Interinstitucional, a la Ley Nº 18.331 y su reglamentación.

DICTAMEN No.		EXPEDIENTE No.
14	2013	2012-2-10-004144

Montevideo, 16 de mayo de 2013

VISTO:

La consulta formulada por el Ministerio de Relaciones Exteriores sobre la adecuación de un Proyecto de Convenio Interinstitucional que presenta ante la Unidad, a la Ley Nº 18.331 y su reglamentación.

RESULTANDO:

I) Que de la lectura del texto propuesto surge el núcleo o propósito esencial del Convenio, consiste en una conexión en modalidad "web service" al Servicio SIDECO que proporciona la Dirección Nacional de Identificación Civil.

II) Que a través de este servicio se facilitaría el contralor de autenticidad de cédulas de identidad de los usuarios que accedan a los diferentes trámites que ofrece el Ministerio, así como la consulta de datos y servicios informáticos.

CONSIDERANDO:

I) Que la Unidad se ha pronunciado antes sobre las características de este Servicio y su adecuación al régimen de la protección de datos personales, a través del Dictamen Nº 32 de 27 de diciembre de 2011 y el Informe Letrado Nº 5934 de 3 de junio de 2011.

II) Que en relación al caso se reitera que la simple visualización electrónica de la información contenida en una cédula de identidad constituye un proceso necesario para validar un acto de identificación, y es conforme al marco regulatorio de la protección de datos personales.

III) Que a mayor abundamiento cabe sostener que el Convenio proyectado cuenta con un marco normativo aceptable (principio de legalidad, art. 6º de la Ley), alude a tratamientos adecuados y no excesivos en relación a la finalidad perseguida (principios de veracidad y finalidad, arts. 7º y 8º de la Ley), y no requiere consentimiento de los titulares de los datos por ingresar dentro de las excepciones previstas (arts. 9º y 17 de la Ley).

IV) Que en cuanto al cuidado de los datos personales en juego, es de orden suponer que ambas partes acordantes, la DNIC y el Ministerio de RR.EE., tomarán las previsiones del caso (principio de seguridad de los datos, art. 10 de la Ley), respetarán la confidencialidad (principio de reserva, art. 11 de Ley), y se atendrán al reacomodamiento de eventuales disfunciones que se produjeran (principio de responsabilidad, art. 12 de la Ley).

V) Que un sistema identificatorio como el consultado no resulta necesariamente justificado, y por tanto legítimo, para todo tipo de trámites, existiendo -además- ciertas aristas del tema vinculadas al derecho de acceso a la información pública, por lo que se sugerirá recabar la opinión de la Unidad de Acceso a la Información Pública.

ATENTO:

A lo precedentemente expuesto, al Informe Letrado que antecede, y a lo dispuesto por los arts. 5º a 12, y 17 lit. B) de la Ley Nº 18.331 y sus modificativas, así como la Ley Nº 18.381.

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

Que el Convenio de conexión “web service” para el contralor de la autenticidad de la cédula de identidad, y la consulta de datos y servicios informáticos, a celebrarse entre el Ministerio de Relaciones Exteriores y la Dirección Nacional de Identificación Civil del Ministerio del Interior, se adecua a lo dispuesto por la Ley Nº 18.331 y su reglamentación, sin perjuicio de lo consignado en el Considerando V del presente.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 15, de 23 de mayo de 2013.

Se dictamina sobre la consulta del Observatorio Uruguayo de Drogas de la Secretaría Nacional de Drogas acerca del plazo máximo de conservación de datos de salud.

DICTAMEN Nº		EXPEDIENTE Nº
15	2013	2011-2-10-0000584

Montevideo, 23 de mayo de 2013

VISTO:

La consulta formulada por el Observatorio Uruguayo de Drogas de la Secretaría Nacional de Drogas acerca de cuál es el plazo máximo de conservación de los datos objeto de estudio por parte del mismo (Exp. N° 2011-2-10 -0000584 ampliación de consulta realizada con anterioridad por la Junta Nacional de Drogas).

RESULTANDO:

I) Que la Junta Nacional de Drogas (JND) es el organismo responsable de la base de datos de usuarios de centros especializados en adicciones.

II) Que la Secretaría Nacional de Drogas (SND) es el soporte técnico-administrativo que tiene por cometido la articulación, coordinación y seguimiento de la aplicación y ejecución de las diferentes acciones surgidas de la JND que competen a los diferentes organismos del Estado.

CONSIDERANDO:

I) Que dicha base cuenta con datos especialmente protegidos, como son los datos de salud, que se encuentran reglamentados en los arts. 18 y 19 de la Ley N° 18.331 (LPDP) y que el art. 4° lit. E) del decreto N° 414/009, reglamentario de la Ley, indica que “dato personal relacionado con la salud refiere a las informaciones concernientes a la salud pasada, presente y futura, física o mental, de una persona”.

II) Que en cuanto al tiempo de conservación, hay que estar a lo establecido en el Principio de Finalidad, art. 8° de la Ley, o sea que los datos no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención y deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. La reglamentación determinará los “casos y procedimientos a los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo a la legislación específica, se conserven datos personales, aun cuando haya perimido tal necesidad o pertinencia”.

III) Que el art. 18 de la Ley, establece que los datos sensibles “también podrán ser

tratados con finalidades estadísticas o científicas cuando se disocien de sus titulares", y en esos casos no sería necesario su eliminación pues la información no puede vincularse a persona determinada o determinable. Asimismo, los arts. 37 y sgtes. del decreto N° 414/009 determinan el procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos.

IV) Que la disposición anterior alude a otro criterio que refiere al tiempo de conservación originado en el valor que puede tener cierta información pública para la sociedad. En este sentido el art. 6° de la Ley N° 18.381 establece la obligación de custodiar la información pública y las responsabilidades que derivan de ello, así como el decreto reglamentario N° 232/010, en los arts. 15 y 16 desarrollan los principios de integridad y de conservación de la información pública.

V) Que a su vez, de acuerdo al art. 3° de la Ley Nº 18.335 de Pacientes y Usuarios de los Servicios de Salud, los usuarios del registro de tratamiento y centros de atención de adicciones de la JND, deben ser considerados pacientes y toda la información que se recabe sobre ellos son datos de salud, pues aluden a algún tipo de tratamiento o atención que refiere a determinada adicción.

VI) Que esta Ley establece una serie de derechos propios de los usuarios del sistema de salud, como por ejemplo elección del sistema asistencial más adecuado, que en caso de cambiar de institución o de sistema de cobertura los datos de salud estén disponibles en forma de historia clínica, derecho de acceso a los resultados cuando así lo solicite, derecho a que se lleve una historia clínica completa, escrita o electrónica, donde figure la evolución de su estado de salud desde el nacimiento hasta la muerte (arts. 7°, 13, 18 lit. D)); así como también consagra la concepción de la historia clínica como conjunto de documentos, no sujetos a alteración ni destrucción, salvo lo establecido en la normativa vigente.

VII) Que por su parte el decreto N° 274/010, reglamentario de la Ley antes citada, establece que los servicios de salud deberán conservar y custodiar las historias clínicas de sus pacientes, sin alterarlas ni destruirlas, de acuerdo a los requisitos y procedimientos establecidos por las disposiciones vigentes. No obstante, la historia clínica escrita, en soporte papel, podrá ser destruida observando los requisitos y procedimientos establecidos por el decreto N° 355/982 de 17 de setiembre de 1982, con las modificaciones introducidas por el decreto N° 37/005 de 27 de enero de 2005.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que por tratarse de datos de salud se aplican los tiempos de conservación y los procedimientos indicados para el tratamiento de la Historia Clínica (Ley N° 18.335, decretos

274/010, 37/005, 396/003 y 355/082).

2. Establecer que también corresponde considerar lo dispuesto en los arts. 8° y 17 lits. C) y D) de la Ley N° 18.331, en la medida que ello no afecte el cometido específico de la Junta Nacional de Drogas como organismo público.

3. Notifíquese, publíquese.

Firmado:
Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 17, de 29 de mayo de 2013.

Se dictamina sobre la consulta relativa a la legalidad del procedimiento de respaldo de información personal e institucional, que se guarda en una computadora personal.

DICTAMEN No.		EXPEDIENTE No.
17	2013	2013-2-10-0000050

Montevideo, 29 de mayo de 2013

VISTO:

La consulta del Sr. Arturo Toscano, acerca de la legalidad del procedimiento de respaldo de la información personal e institucional que guardaba en la computadora que utilizaba en el trabajo.

RESULTANDO:

Que se trata de un funcionario que utiliza una PC institucional y un servidor de correo Outlook, tanto para sus actividades personales como laborales.

CONSIDERANDO:

I) Que corresponde analizar el derecho del funcionario a la privacidad y a protección de sus datos personales en el ámbito laboral, así como la potestad de control y de discrecionalidad que posee la administración pública en el ámbito de sus funciones, con relación a las actividades desarrolladas por éste, así como de sus recursos.

II) Que el respaldo de la información de su PC ha sido realizado por la Dirección Nacional de Innovación, Ciencia y Tecnología (DICyT), dirección dependiente del MEC, creada por la Ley N° 17.930 con el cometido de elaborar e impulsar las políticas, lineamientos, estrategias y prioridades del Ministerio en materia de innovación, ciencia y tecnología.

III) Que respecto a la pertenencia del correo otorgado al trabajador, es clara la jurisprudencia laboral en cuanto a considerar que es una herramienta y un recurso propio del empleador, entregado en tal carácter para que se cumpla con las tareas asignadas.

IV) Que además hay que tener presente que los tribunales laborales han entendido que, más allá de la debida protección de la intimidad y la privacidad de los trabajadores, hay un margen de control al que tienen derecho los empleadores.

V) Que por otra parte, si bien no ha existido un consentimiento expreso se puede inferir que el mismo está implícito en la relación laboral que se mantiene con el organismo, además de que el art. 9° B) de la Ley establece que no se requiere el consentimiento cuando los datos se recaben para el ejercicio de las funciones propias de los poderes del Estado o en virtud de una obligación legal.

VI) Que no obstante ello, cada responsable de base de datos o de tratamiento de datos, está obligado a adoptar medidas de seguridad para proteger adecuadamente los datos

personales que posee (arts. 10, 11 y 12 de la Ley N° 18.331).

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que no se ha vulnerado la Ley N° 18.331, ya que la actuación del Ministerio de Educación y Cultura se enmarca en los principios de finalidad, necesidad y proporcionalidad en el cumplimiento de sus funciones (art. 9° lit. B).

2. Establecer que el consentimiento del consultante es parte de la relación contractual según lo expresado en el art. 9° lit. D).

3. Establecer asimismo que es obligación del organismo utilizar esa información sólo para la finalidad para la cual ha sido recabada según lo establecido en el art. 8º de la Ley, así como que deberá garantizar la seguridad y confidencialidad de los mismos.

4.- Notifíquese, publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 19, de 29 de mayo de 2013.

Se dictamina sobre la consulta formulada por el Director del Programa Salud.uy sobre la procedencia de comunicar datos personales de profesionales para incluir en el catálogo que llevará el Ministerio de Salud Pública.

DICTAMEN Nº		EXPEDIENTE Nº
19	2013	2013-2-10-0000177

Montevideo, 29 de mayo de 2013

VISTO:

La consulta formulada por Jorge Forcella sobre comunicación de datos de profesionales a incluir en el catálogo del Ministerio de Salud Pública (MSP), en el marco del Proyecto E-Salud.

RESULTANDO:

Que la finalidad es estandarizar los diferentes códigos utilizados en el área para que los prestadores de salud puedan construir historias clínicas electrónicas interoperables, y que entre dichos catálogos se encuentra el de los profesionales de la salud habilitados por el MSP.

CONSIDERANDO:

I) Que se trata de la comunicación de ciertos datos personales de profesionales de la salud (Cédula de Identidad, nombres y apellidos, fecha de nacimiento, sexo, si es profesional médico o no, si está habilitado a ejercer o no, número de caja profesional), a los Efectores del Sistema Nacional Integrado de Salud – SNIS (prestadores de servicios públicos y privados que integran el sistema).

II) Que la Ley N° 18.211 sobre el Sistema Nacional Integrado de Salud, establece en el art. 2° que compete al Ministerio de Salud Pública la implementación del sistema que articulará a los prestadores públicos y privados de atención integral a la salud.

III) Que el art. 17 establece que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos.

IV) Que en el caso es perfectamente aplicable lo antes expresado, pues es de su interés del MSP cumplir con los cometidos legales asignados por la Ley a efectos de garantizar el funcionamiento del Sistema, así como en cuanto a los profesionales, es de su interés que sus servicios sean contratados, para lo cual es necesario que cierta información, tanto la relativa a la identidad como a la referida a sus acreditaciones profesionales, sean conocidos por quienes operan en el sistema.

V) Que además aplica al caso la hipótesis considerada por la Ley respecto a que así lo disponga una ley de interés general, pues en el caso existen normas habilitantes como la Ley N° 18.211 y la Ley N° 18.335, entre otras.

VI) Que la anterior excepción se relaciona también con las establecidas en el art. 9° lit. B) y lit. C), respecto a que no se requiere solicitar el consentimiento cuando los datos se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, ni cuando se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que el MSP no requiere recabar el previo consentimiento informado de los profesionales de la salud, para comunicar los datos en el marco de las obligaciones establecidas en la Leyes N° 18.211 y Nº 18.335, pues aplican al caso las excepciones previstas en el los art. 9° lits B), C) y D), y 17 lits A) y B) de la Ley N° 18.331.

2. Notifíquese, publíquese.

Firmado:

Dr. Felipe Rotondo
Consejo Ejecutivo URCDP

Dictamen Nº 21, de 4 de julio de 2013.

Se dictamina sobre la consulta relativa a la adecuación de una base de datos de recomendaciones empresariales al marco legal establecido por la Ley Nº 18.331.

DICTAMEN Nº		EXPEDIENTE Nº
21	2013	2013-2-10-0000219

Montevideo, 4 de julio de 2013

VISTO:

La consulta formulada por el Sr. Guillermo Winkler sobre adecuación de su base de datos de recomendaciones empresariales al marco legal establecido por la Ley N° 18.331.

RESULTANDO:

Que se trata de un sistema de referencias empresariales, donde cada empresa afiliada, podrá ingresar cédula y nombre del empleado y una evaluación numérica que indique si lo recomienda o no lo recomienda.

CONSIDERANDO:

I) Que para poder consultar las referencias incluidas en el sistema, las empresas deberán estar afiliadas y obtener el consentimiento previo de las personas, que les proveerán con cédula de identidad para que se pueda realizar la búsqueda. Además el sistema no permite emitir listados ni navegar la información de personas que no hayan brindado el consentimiento para la consulta.

II) Que el art. 17 de la Ley establece que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos.

III) Que en el caso, si bien existe interés legítimo del emisor y del destinatario, no se puede inferir el consentimiento del trabajador del contexto de la relación laboral o contractual, ni por la entrega de la CI, pues el sistema que instituye la Ley no se basa en el consentimiento tácito sino en el consentimiento expreso (art. 9° primera parte).

IV) Que en este sentido, si bien el art. 9° lit. D) de la Ley establece la excepción al consentimiento cuando los datos deriven de una relación laboral o contractual, y sean necesarios para su desarrollo o cumplimiento, en el caso hay que diferenciar entre la relación en sí, y la posibilidad de ser incluido en esta base de datos de referencias empresariales, pues esto último no es necesario para el desarrollo o cumplimiento de la relación de que se trate, -exigencia prevista en el art. 9° lit. D)-, por ende, debe solicitarse el consentimiento en forma expresa, ya sea mediante un formulario o una cláusula específica.

V) Que por otra parte, los trabajadores cuyos datos van a ser ingresados en el sistema

y eventualmente comunicados, deben ser informados de la finalidad de la base y de esa eventual comunicación, en los términos establecidos en el art. 13 de la Ley.

VI) Que considerando lo establecido en el art. 7° de la Ley, la recomendación en sí deberá ser lo más objetiva posible, sin juicios de valor que puedan vulnerar la integridad de las personas, y sin la inclusión de datos sensibles que puedan constituirse en una forma de discriminación, así como la recolección de estos datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a la Ley.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que debe recabarse el consentimiento en forma expresa mediante un formulario o cláusula específica que debe ser firmada por los trabajadores, conforme lo establecido en el art. 9° de la Ley.

2. Establecer además que deberán ser informados en los términos previstos en el art. 13 de la Ley, así como el responsable de la base deberá adoptar las medidas de seguridad adecuadas, e inscribir la base de datos en el registro de la URCDP, dentro de los 90 días siguientes a su creación.

3. Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 22, de 4 de julio de 2013.

Se dictamina sobre consulta de la Intendencia de Montevideo sobre la inclusión en el sitio web de los datos del índice de archivo del Servicio de Registro Civil con carácter de dato abierto.

DICTAMEN No.		EXPEDIENTE No.
22	2013	2013-2-10-0000130

Montevideo, 4 de julio de 2013

VISTO:

La consulta de la Intendencia de Montevideo sobre la inclusión en el sitio web de datos del índice de archivo del Servicio de Registro de Estado Civil.

RESULTANDO:

Que se considera la posibilidad de publicar en la web institucional el índice de archivo del Servicio de Registro de Estado Civil, con carácter de "dato abierto", pues los datos a los que podría accederse con esta publicación, no son datos que requieren previo consentimiento informado

CONSIDERANDO:

I) Que los datos serían los siguientes: nombre completo de la persona y su fecha de nacimiento, matrimonio o defunción, con referencia al Año, Sección y Número de Acta, sin asociar la imagen de la partida de que se trate.

II) Que respecto al carácter de "dato abierto", corresponde mencionar que el criterio aplicado por la IM, -y plenamente compartido-, siempre ha consistido en asegurarse que los datos que publica con este carácter sean efectivamente públicos, en definitiva que no se trate de información reservada, confidencial o secreta, según lo establecido en la Ley N° 18.381 de Acceso a la Información Pública y en la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data.

III) Que en nuestro país, de acuerdo con la Ley N° 18.331, cualquier iniciativa de datos abiertos debe considerar el anonimato de personas tanto físicas como jurídicas, pues el art. 4° de esta Ley establece que dato personal se trata de información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

IV) Que el art. 9 lit. C) de esta norma indica que el tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse, agregando que éste será necesario el previo consentimiento cuando: C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, por lo tanto algunos de los datos que se van a publicar no están incluidos en este listado.

V) Que la función del Registro de Estado Civil es anotar los hechos o actos que atañen

al estado civil, con la intervención de un funcionario público competente (Oficial del Estado Civil) en los libros correspondientes y con las formalidades que la ley prescribe.

VI) Que por ende esto debe estar en consonancia con lo establecido en el art. 17 de la Ley que indica que la comunicación de datos personales objeto de tratamiento, sólo podrá realizarse para cumplir con los fines directamente relacionados con el interés legítimo del emisor y del destinatario, con el previo consentimiento del titular, salvo que así lo disponga una ley de interés general o en los dispuestos del art. 9° (por ejemplo los listados), o los datos sean disociados (anonimizados).

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que la publicidad de determinados datos personales, como los datos de matrimonio o de defunción, sin el consentimiento del titular, vulneran las disposiciones de la Ley N° 18.331.

2. Establecer que el tratamiento de estos datos debe ajustarse a los principios de proporcionalidad (art. 7°) y de finalidad (art. 8°), así como a lo establecido en los arts. 9° y 17 lit. A), por lo que el índice debería publicarse sin los datos antes indicados o sin identificar a sus titulares (art. 17 lit. D) de la Ley citada).

3. Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 25, de 1 de agosto de 2013.

Se dictamina sobre consulta formulada por el Jefe de la Oficina de Información Pública y Datos Personales de la Administración de Obras Sanitarias del Estado (OSE) sobre la constancia de deuda que el organismo otorga a solicitud de usuarios, mediante el llenado de un formulario que contiene datos personales.

DICTAMEN No.		EXPEDIENTE No.
25	2013	2012-6-1-0000853

Montevideo, 1 de agosto de 2013

VISTO:

La consulta formulada por el Esc. Horacio Uran, Jefe de la Oficina de Información Pública y Datos Personales de OSE, referida a la constancia de deuda que este organismo otorga a solicitud de los usuarios, mediante el llenado de un formulario que contiene datos personales de acuerdo a la definición del art. 4 inc. D) de la Ley N°18.331.

RESULTANDO:

I) Que esos datos refieren al bien y al titular del servicio contratado, así como la relación entre ambos y la existencia en su caso, de una deuda de este último.

II) Que el consultante entiende que para comunicar dichos datos existe interés legítimo por parte de OSE, pues se trata de una de las competencias que le ha sido adjudicada en la Ley Orgánica N° 11.907, pero se presenta la duda respecto al interés legítimo del solicitante del certificado (destinatario), respecto a si es necesario o no la acreditación del interés legítimo de su parte, salvo tratándose del titular de la deuda o de quien este autorice.

III) Que respecto al consentimiento, el Esc. Uran entiende que se trata de una comunicación por parte de OSE a terceros donde opera la excepción establecida al mismo en el lit. B) del art. 9º de la Ley 18331 por remisión del lit. B) del art. 17 de dicha norma, o sea es “el ejercicio de funciones propias de los poderes del Estado”. También se entiende que no es de aplicación el art. 22 de la Ley por cuanto no estamos en el Ente ante la actividad que regula el mismo y en las condiciones que establece.

CONSIDERANDO:

I) Que según lo establecido en la Ley N° 18.331 art. 9° lit. C), existen determinados datos personales que no requieren para su tratamiento el previo consentimiento del titular, en el caso de personas físicas: nombres y apellidos, documento de identidad, domicilio, nacionalidad y fecha de nacimiento y respecto a las personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de los responsables.

II) Que por otra parte, el lit. B) del art. 9° establece que no es necesario recabar el previo consentimiento informado, cuando se está ante el “ejercicio de funciones propias de

los Poderes del Estado", o la recolección de datos se efectúa "en virtud de una obligación legal", hipótesis que refiere al ámbito de la recolección de datos, o sea cuando los datos de los clientes son recabados por parte de OSE para brindar sus servicios.

III) Que en ese sentido, tomando en consideración los cometidos inherentes a OSE y su marco legal, cabe inferir que no es necesario recabar el consentimiento de los clientes a efectos de cumplir con sus funciones o cometidos, así como para comunicar esos datos a determinados organismos públicos, siempre y cuando ello se corresponda con las funciones o cometidos de cada uno de éstos, a la finalidad del intercambio y a la regulación legal de dicho funcionamiento (arts. 157 a 160 de la Ley N° 18. 719 de 27 de diciembre de 2010).

IV) Que ello no significa que puedan comunicarse datos personales que requieren previo consentimiento a terceros ajenos (particulares que no acreditan ningún interés legítimo). En este caso comunicar a terceros que el titular tenga una deuda y el monto de la misma, excede el ámbito de aplicación del art. 9º lit. C), y además no forma parte del interés del cliente de OSE a la hora de brindar sus datos al organismo público.

V) Que en definitiva, se debería aplicar un procedimiento de disociación (art. 17 lit. D) de la Ley N° 18.331), de forma tal que la información o el asunto no pueda vincularse a persona determinada o determinables, salvo que quien lo solicite sea el propio titular, su representante o herederos, o de contrario configurar un formulario similar al que se utiliza para entregar información a los profesionales escribanos (solicitud libre de deuda), quienes deben indicar el interés legítimo.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1.Indicar que corresponde la disociación de los datos personales o la reformulación del formulario de forma tal que conste el interés legítimo de tal solicitud.

2. Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 26, de 8 de agosto de 2013.

Se dictamina sobre consulta realizada por la Comisión de Protección de Datos Personales de la Contaduría General de la Nación sobre el alcance de las palabras “listados” y “medios” utilizados en el artículo 9 C) de la Ley Nº 18.331 y en los artículos 3 B) y 9 D) del Decreto Nº 414/009.

DICTAMEN No.		EXPEDIENTE No
26	2013	2013-2-10-0000230

Montevideo, 8 de agosto de 2013

VISTO:

La consulta realizada por la Comisión de Protección de Datos Personales de la Contaduría General de la Nación, sobre el alcance de las palabras “listados” y “medios”, utilizadas en el art. 9º lit. C) de la Ley N° 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data, y del art. 3º lit. B) del decreto N° 414/009 de 31 de Agosto de 2009, así como sobre la exigencia de motivación para el ejercicio de los derechos, solicitada en el art. 9º lit. D) del mismo decreto.

CONSIDERANDO:

I) Que en la especie resultan de aplicación las reglas de interpretación de la Leyes, establecidas en el Título Preliminar del Código Civil.

II) Que las palabras “listados” y “medios”, no han sido definidas expresamente por el legislador en materia de protección de datos personales, por lo que deben ser entendidas en sus sentidos naturales y obvios, según el uso general.

III) Que según lo expresado por esta Unidad en Resolución N° 750/2010 de 18 de Julio de 2010, el art. 9º lit. D) del decreto establece criterios a seguir por el titular del dato al ejercitar su derecho de acceso, que en forma alguna pueden considerarse como una formalidad que pueda ser exigida por el responsable de la base de datos.

ATENTO:

A lo expuesto, y a lo previsto por los arts. 31 y 34 de la Ley N° 18.331,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Expedirse en el sentido que las palabras “listados” y “medios” utilizadas en el art. 9º lit. C) de la LPDP y art. 3º lit. B) del decreto N° 414/009, deben ser entendidas en sus sentidos naturales y obvios, según el uso general.

2. Que el art. 9º lit. D) del decreto establece criterios a seguir por el titular del dato al ejercitar su derecho de acceso, que en forma alguna pueden considerarse como una formalidad que pueda ser exigida por el responsable de la base de datos.

3. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Monteverde

Consejo Ejecutivo URCDP

Dictamen Nº 27, de 8 de agosto de 2013.

Se dictamina sobre consulta formulada por la Dirección de Asuntos Jurídicos y Notariales de la Dirección Nacional de Aduana acerca del carácter de confidencialidad que poseen los datos personales de firmas pertenecientes a empresas despachantes de aduana, cuyo acceso está permitido a terceros a través del Sistema Lucía.

DICTAMEN No.		EXPEDIENTE No.
27	2013	2011/05007/21529

Montevideo, 8 de agosto de 2013

VISTO:

La consulta formulada por la Dirección de Asuntos Jurídicos y Notariales de la Dirección Nacional de Aduanas (en adelante DNA), acerca del carácter de confidencialidad que eventualmente poseen los datos personales de firmas pertenecientes a despachantes de aduana (empresas), cuyo acceso está permitido a terceros a través del Sistema Lucía.

RESULTANDO:

I) Que en un primer informe se le indica a la DNA que "si bien no está obligada a obtener el consentimiento para recabar los datos contenidos en el DUA o en otros documentos necesarios para dar trámite a las importaciones y exportaciones; así como tampoco para comunicarlos a determinados organismos públicos en el marco de sus competencias y funciones, sí debería atenderse a la confidencialidad que puede revestir cierta información comercial de las empresas, así como de datos personales que requieren el previo consentimiento del titular para ser comunicados a terceros".

II) Que en forma posterior la DNA solicita a la Unidad que se amplíe el referido informe en lo relativo al carácter de la "confidencialidad que puede revestir cierta información comercial de las empresas, así como de aquellos datos personales que sí requieren el previo consentimiento del titular a efectos de ser comunicados a terceros".

III) Que a su vez la DNA indica que se brinda acceso a la siguiente información: RUT, nombre de despachante y datos del DUA que incluyen: nombre y RUT del importador, datos de la mercadería (declaración arancelaria, valor, cantidad, ajustes, descripción comercial, origen, procedencia), tributos a pagar, pagados, documentos, certificados asociados al DUA (emitidos por otros organismos que intervienen en la operación de comercio exterior, como Ministerios, LATU, licencias, certificados de origen, transportista, datos del contenedor).

CONSIDERANDO:

I) Que considerando los cometidos inherentes a la DNA y su marco legal, no es necesario recabar el consentimiento de los involucrados o interesados, a efectos de cumplir con sus funciones o cometidos (art. 9° lit. B), así como tampoco para comunicar ciertos datos a determinados organismos públicos, siempre y cuando ello se corresponda con las funciones

o cometidos de cada uno de éstos, a la finalidad del intercambio y a la regulación legal del mismo (arts. 157 a 160 de la Ley N° 18. 719 de 27 de diciembre de 2010).

II) Que de acuerdo con la Ley N° 18.331 hay datos personales de las empresas (art. 2°) que requieren el previo consentimiento informado para ser comunicados (art. 9°), por lo cual algunos de los que se mencionan (clientes, volumen comercial, cantidades de operaciones que realiza, etc.), requieren del mismo para la publicación; además de que es necesario tener presente que esa información también puede entregarse con carácter de confidencial, por parte de las empresas a la DNA, de acuerdo con lo establecido en el art. 10° de la Ley N° 13.381 de Acceso a la Información Pública.

III) Que en este sentido, algunos campos del DUA contienen datos identificatorios, como nombre y número de RUT del importador, nombre de la empresa que actúa como despachante de aduana, nombre de la empresa que brinda los servicios logísticos requeridos, RUT de la empresa transportista y dirección del destinatario; pero otros campos incluyen información de tipo económica, así como información relativa a los tributos que gravan la operación y sus montos que puede ser considerada confidencial o se trata de datos que no integran el listado del art. 9° lit. C).

IV) Que en definitiva, las soluciones desde el punto de vista de la protección de datos, pueden ser las siguientes: a) recabar el consentimiento de las empresas a efectos de que esa información se pueda brindar a través del Sistema Lucía según lo establecido en el art. 9°; b) publicar sólo los datos que se mencionan en el listado del art. 9° lit. C), o c) que los datos vinculados a las operaciones comerciales se publiquen pero disociados de los titulares, según lo establecido en el art. 17 lit. D).

V) Que sin embargo, ninguna de estas soluciones implica que la DNA no pueda recabar de los interesados los datos, o comunicar la información en forma completa, -incluida la que requiere el previo consentimiento informado-, a determinados organismos públicos (como el LATU, los Ministerios, etc.) en el cumplimiento de sus funciones (arts. 9 B)17 A y B)).

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA:

1. Indicar que en el caso de datos que requieren el previo consentimiento informado, corresponde recabar el mismo (art. 9° y 17), o aplicar un mecanismo de disociación (art. 17), o de lo contrario la publicación de la DNA debería limitarse sólo a los datos incluidos en el listado del art. 9° lit. C).

2. Establecer que la DNA no requiere de dicho consentimiento para recolectar dichos datos o para comunicar la información en forma completa a determinados organismos públicos en el marco del cumplimiento de sus funciones (arts. 9º lit. B) y 17 lits. A) y B).

3. Notifíquese, publíquese.

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo URCDP

Dictamen Nº 29, de 24 de octubre de 2013.

Se dictamina sobre consulta formulada por la Secretaría del Departamento de Informática del Ministerio del Interior acerca de la información digital almacenada en los chips para el proyecto de cédula de identidad electrónica.

DICTAMEN No.		EXPEDIENTE No.
29	2013	2013-2-10-0000391

Montevideo, 24 de octubre de 2013

VISTO:

La consulta formulada por la Ing. Sabrina Trotta Mouriño de la Secretaría del Departamento de Informática del Ministerio del Interior (MI).

RESULTANDO:

I) Que el MI trabaja en la elaboración del pliego de un proyecto que comprende la inclusión de una cédula de identidad electrónica (CIE), con el objetivo es que la misma sea un documento de viaje conforme al ICAO 9303.

II) Que dicha CIE presentará información visible (como hasta ahora) e información digital almacenada en chips de dos tipos: uno con contacto y otro sin contacto. El chip con contacto para ser leído requiere de un dispositivo de lectura, mientras que el chip sin contacto puede ser leído con un dispositivo de lectura autorizado a una distancia máxima de 10 cm entre lector y CI.

III) Que se consulta acerca de que datos se pueden o no, almacenar en el chip sin contacto, considerando que el ICAO 9303 ha determinado como obligatorios los siguientes: tipo de documento, Estado u organismo expedidor, nombre (del titular), número de documento, dígito de control - número de documento, nacionalidad, fecha de nacimiento, dígito de control - fecha de nacimiento, sexo (de nacimiento (N) y sexo actual (A), en formato N/A), fecha de expiración o válido hasta y rostro. Las principales dudas surgen con los datos relativos al sexo y al rostro.

CONSIDERANDO:

I) Que de acuerdo con la Ley N° 18.331, arts. 18 y 19, hay datos personales que requieren de una protección especial para ser tratados y almacenados, por considerarse datos sensibles.

II) Que no obstante ello corresponde tener presente que existen obligaciones a cargo de los Estados, que implican instrumentar las medidas necesarias y adecuadas, para garantizar y proteger los derechos humanos de todas las personas, incluyendo la seguridad pública.

III) Que en este sentido el art. 18 que establece que los “datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo.”

IV) Que se infiere de la consulta que se trata de cumplir con las funciones que posee el MI en materia de seguridad pública, para lo cual es necesario identificar en forma certera y precisa, a todas las personas, especialmente en lugares de entrada y salida del país como los aeropuertos.

V) Que se indica en la consulta que los datos solicitados se enmarcan en el Documento ICAO 9303 que se trata de un material elaborado por la Organización de Aviación Civil Internacional, que recomienda las características que deben tener los documentos de viaje de lecturas mecánicas.

VI) Que en cuanto al rostro, cabe destacar que se trata de un dato biométrico así como el reconocimiento facial, se trata es una aplicación dirigida por un programa informático, destinado a identificar automáticamente a una persona en una imagen digital, mediante la comparación de determinadas características faciales existentes en una base de datos, por lo cual se recomienda su uso al sólo efecto de dicha verificación.

VII) Que en razón de ello, los elementos biométricos en los pasaportes, en otros documentos de viaje o en los carnés de identidad son muy sensibles, por lo cual debe garantizarse que sólo las autoridades competentes pueden acceder a los datos almacenados en el chip.

VIII) Que lo delicado del tema obliga a utilizar sistemas seguros, que entre otras cosas, impidan que se memoricen los rostros por parte de terceros no autorizados, que el acceso a las imágenes de reconocimiento facial esté restringido sólo a las autoridades competentes, así como debe utilizarse una arquitectura de seguridad que proporcione un nivel adecuado para el intercambio de dicha información, como por ejemplo, una Infraestructura de Clave Pública Global (PKI), que afortunadamente Uruguay ya posee (Ley N° 18.600 de Documento y Firma Electrónica y su Decreto 436/011 de 8 de diciembre de 2011.

IX) Que en definitiva, si bien el art. 3° de la Ley N° 18.331, indica que las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado, quedan excluidas de su ámbito de aplicación, corresponde que desde la perspectiva de un derecho humano como lo es la protección de datos personales, se consideren las recomendaciones formuladas por la URCDP.

ATENTO:

A lo dispuesto en las normas antes citadas,

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA

1. Recomendar al MI que restrinja el acceso a datos de sexo y de rostro, solamente a las autoridades competentes, así como que la recolección y almacenamiento de los mismos, se realicen a los solos efectos de la seguridad pública, en el marco del cumplimiento de las funciones y cometidos que posee dicho Ministerio, en consonancia con los principios de Finalidad y Proporcionalidad previstos en la Ley N° 18.331.

2. Notifíquese, publíquese y oportunamente archívese.

Firmado:

Mag. Federico Montevideo
Consejo Ejecutivo de la URCDP

Dictamen Nº 30, de 24 de octubre de 2013.

Se dictamina sobre consulta relativa a la existencia de mecanismos de control sobre plazos de conservación de los datos de carácter objetivo.

DICTAMEN No.		EXPEDIENTE No.
30	2013	2013-2-10-0000029

Montevideo, 24 de octubre de 2013

VISTO:

La consulta formulada por el Sr. Luis Edgardo Olivera, acerca de la existencia de mecanismos de control sobre plazos de conservación de los datos de carácter objetivo, así como lo que sucede en caso de que existan inscripciones sucesivas en diferentes bases de datos de este tipo.

RESULTANDO:

Que las bases de datos que brindan información comercial de carácter objetivo, se nutren con los datos informados por las entidades adheridas a determinadas empresas especializadas en el tema, responsables de las mismos y que brindan ese servicio, así como también se pueden conformar con datos obtenidos de fuentes de acceso público.

CONSIDERANDO:

I) Que la legalidad, respecto a los datos, objeto de recolección y tratamiento, se encuentra regulada en forma explícita en la Ley N° 18.331, art.22.

II) Que el contenido de dichas bases, debe estar únicamente referido a la “solvencia patrimonial o crediticia”, de forma tal que se pueda determinar la solvencia económica actual del interesado, por ello es muy importante que se ajusten a los principios de finalidad, proporcionalidad y calidad de la información.

III) Que por el momento sólo existen dos formas de control: a) el que puede realizar el interesado o titular perjudicado por este tipo de registro, a través del ejercicio de los derechos que se consagran en la Ley (arts. 14 y 15), y b) el control que realiza la URCDP, como Órgano Regulador que tiene a su cargo la tuición del tratamiento de los datos personales en sentido amplio, incluido el control de lo establecido en el art. 22 con plena competencia para ello.

IV) Que respecto al control de la URCDP, cabe tener presente que toda persona física o jurídica que posea una base de datos de este tipo tiene la obligación de inscribirla en el registro (art. 28 de la LPDP), por ende la Unidad realiza el control correspondiente cuando la base se inscribe, contrastando la información que se proporciona con lo establecido en la Ley, así como también cuando se reciben consultas o denuncias de particulares.

V) Que por otra parte, el Consejo Ejecutivo de la URCDP tiene potestades sancionatorias ante el incumplimiento de la LPDP, pudiendo imponer sanciones de apercibimiento, multa de hasta quinientas mil unidades indexadas y clausura de las bases de datos por un plazo de

hasta seis días hábiles (art. 35 de la LPDP).

VI) Que respecto a la posibilidad de inscripción sucesiva, el acreedor puede inscribir en diferentes bases al deudor, pero si ello no se ajusta a la realidad o si es incorrecto incurrirá en responsabilidad, por lo cual tiene obligación de controlar la veracidad de los datos y los plazos, así como tener presente el derecho a inscribir sólo por una vez más, si pasado el plazo de 5 años inicial, la deuda se mantiene impaga.

ATENTO:

A lo dispuesto en las normas antes citadas

EL CONSEJO EJECUTIVO DE LA UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES DICTAMINA

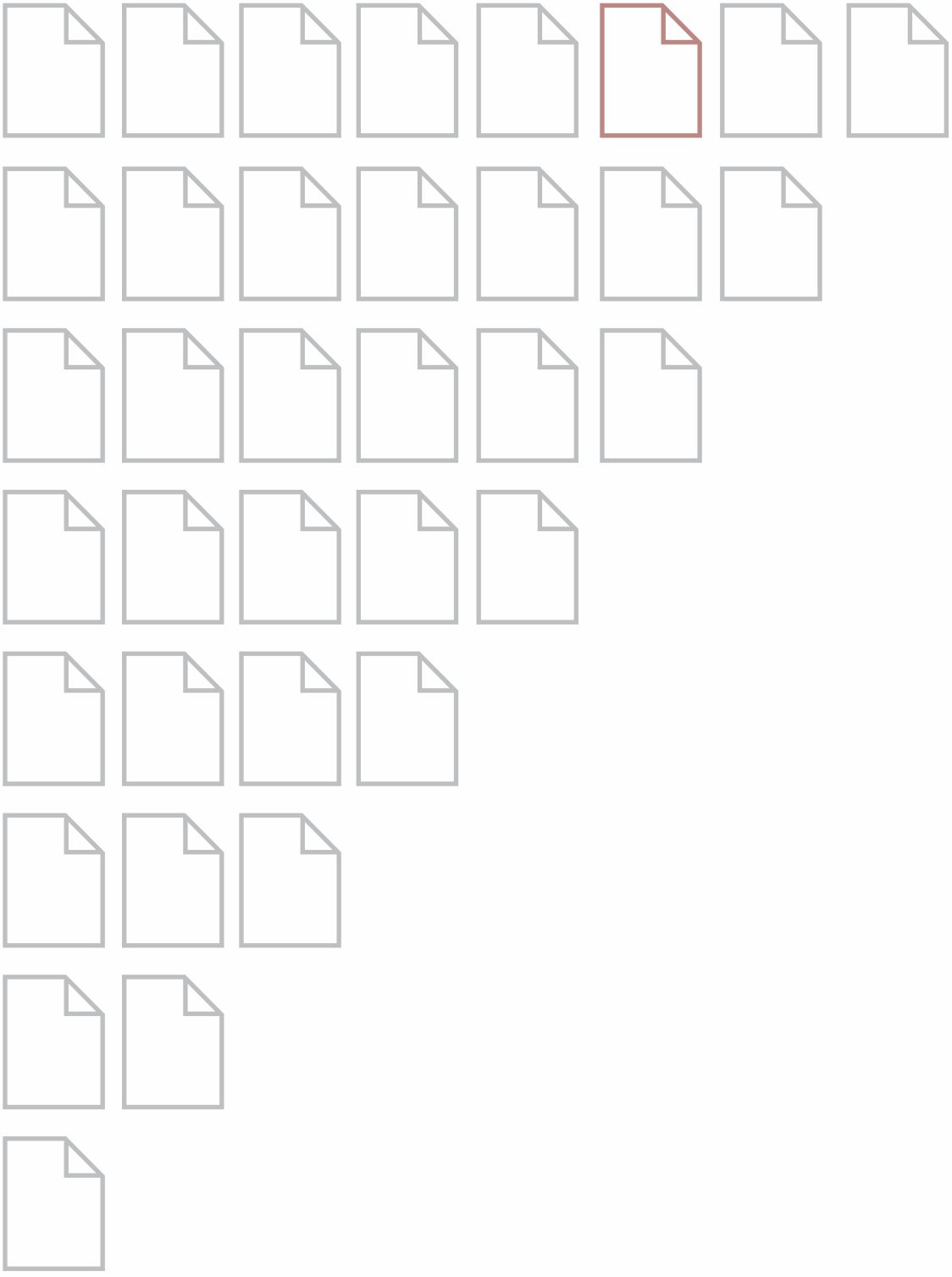
1.Informar al consultante que la legalidad, respecto al objeto de la recolección y tratamiento de estos datos se encuentra regulada en forma explícita en art. 22 de la Ley, así como existen mecanismos de control, tanto a cargo de los propios interesados a través del ejercicio de los derechos que se consagran en la Ley (arts. 14 y 15), y b), como a cargo de la URCDP, Órgano Regulador que tiene a su cargo la tuición del tratamiento de los datos personales en sentido amplio.

2.- Notifíquese, publíquese

Firmado:

Mag. Federico Monteverde
Consejo Ejecutivo de la URCDP

Informes



Informe Nº 10, de 21 de enero de 2013.

Se informa sobre consulta relativa a la legalidad de una comunicación de datos realizada con la finalidad de mejorar la asistencia a los pacientes.

INFORME No.		EXPEDIENTE No.
10	2013	2012-2-10-0000970

Montevideo, 21 de enero de 2013

I. Introducción

La Comisión Honoraria de Salud Renal formula consulta a la Unidad Reguladora y de Control de Datos Personales (URCDP) acerca del alcance de la Ley N° 18.331, en virtud de que cuenta con un Registro Único de Pacientes con Enfermedad Renal Crónica cuya base se asienta en el Fondo Nacional de Recursos, bajo la responsabilidad de la Comisión Honoraria de Salud Renal.

En virtud de la consulta recibida y en cumplimiento de las facultades que le son otorgadas la URCDP por el art. 34 de la Ley, la Unidad procede a la sustanciación de ésta.

II. Análisis de la consulta desde la Ley Nº 18.331

La Ley N° 18.331 regula en forma específica los datos sensibles entre los cuales incluye los datos de salud, para cuyo tratamiento se requiere el consentimiento expreso y escrito de su titular.

Específicamente en lo que respecta a datos relativos a la salud, el art. 19 indica que: “Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley”. De acuerdo a ello, el tratamiento de los datos de salud que constan en el Registro por parte de los médicos nefrólogos es legítimo e inherente a la atención médica que brindan.

La consulta presentada refiere al caso de una comunicación de datos de los pacientes del grupo, ingresados en el Registro, al médico nefrólogo responsable de éste. La finalidad de dicha comunicación es mejorar la asistencia de los pacientes facilitando la identificación de los casos en riesgo.

Por otra parte, es de resaltar que el Programa de Salud Renal cuenta con un formulario para la obtención del consentimiento informado de los pacientes a los efectos de integrar el Registro de Enfermedad Renal Crónica. Es en dicha instancia es pertinente comunicar a los pacientes la posibilidad de que exista una comunicación de sus datos personales en cumplimiento de lo dispuesto por el art. 13 de la Ley. Ello sin perjuicio de lo expresado en el

lit. D) del art. 9° de la Ley Nº 18.331 que prevé las hipótesis en que no se requiere el previo consentimiento del titular de los datos. Para el caso objeto de análisis: “Cuando deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento”. Así, no se requeriría el previo consentimiento de los pacientes para comunicar los datos a los médicos nefrólogos.
Igualmente en los casos de que puedan presentarse situaciones dudosas respecto a los datos que trata la consultante se debe tener presente la naturaleza sensible de los datos de salud y tomarse como rectores los principios generales en materia de protección de datos personales consagrados en el art. 5° y siguientes de la Ley N° 18.331.

III. Conclusiones.

En virtud de lo informado se considera legítima la comunicación de datos que ha motivado la consulta. Se recomienda que frente a situaciones dudosas, se tenga presente la naturaleza sensible de los datos de salud y los principios en materia de protección de datos personales.

Firmado:
Dra. Jimena Hernández
Derechos Ciudadanos

Informe Nº 12, de 26 de febrero de 2013.

Se informa sobre consulta relativa a si puede considerarse de carácter confidencial determinada información.

INFORME No.		EXPEDIENTE No.
12	2013	2011-2-10-0000649

Montevideo, 26 de febrero de 2013

La Unidad de Acceso a la Información Pública remite la consulta que le formulara la Dirección Nacional de Medio Ambiente, DI.NA.MA., a efectos de dictaminar a si la entrega de la información objeto de consulta puede considerarse “información confidencial”, al amparo del nal. II de art. 10 de la Ley de Acceso a la Información Pública: datos personales que requieran previo consentimiento informado.

Se trata, en el caso, de información que presentan las empresas a la citada repartición estatal, atinente a sus respectivos IAO (Índice Ambiental de Operación), volúmenes de agua que utilizan, tipo de fuente (OSE o propia), y efluentes.

Esta información, a su vez, es requerida por otras empresas u organismos estatales, y de ahí el motivo de la consulta elevada a la U.A.I.P. por parte de DINAMA, para saber si está o no autorizada a entregar tal especie de información.

Del punto de vista de las competencias de la Unidad Reguladora y de Control de Datos Personales, en opinión del suscrito deben tenerse en cuenta tres encuadres legales:

1º) El encuadre suministrado por el art. 4º lit. D) de la Ley Nº 18.331, que define lo que es un “dato personal” asumiendo por tal la “información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables”.

Los amplios términos de la definición legal hacen que se aplique sin mayores exigencias a la hipótesis en consulta. O sea que el IAO y las restantes informaciones especificadas son datos personales, o al menos tienen potencialidad como para serlos.

2º) El encuadre proveniente del art. 9º de la Ley Nº 18.331, que sienta como regla general la exigencia del consentimiento del titular para recolección y tratamiento de sus datos, incluyendo la comunicación a terceros.

Las excepciones a esta regla están contempladas en el inciso 3º lits. A) a E) de este último artículo (redacción dada por art. 156 de la ley Nº 18.719), fincándose en la proveniencia del dato o la calidad del sujeto que lo va a tratar, a saber:

A) Fuentes públicas de información.

B) Funciones de poderes del Estado u obligación legal.

C) Listados identificatorios (no incluye número telefónico de persona física).

D) Relación contractual, científica o profesional con el titular de los datos.

E) Uso por persona física para fin exclusivo personal, individual o doméstico.

Con los datos aportados en la consulta no es posible sentar un criterio general, que aplique inexorablemente a los distintos escenarios que pueden abrirse. En términos concretos, una Intendencia Municipal está facultada a obtener la comunicación de este tipo de datos de parte de la DI.NA.MA., acudiendo -con criterio amplio pero fundable al fin- a la excepción del lit. B), que el art. 17 de la misma Ley traslada al ámbito de las cesiones de datos. Sin embargo ni la DI.NA.MA. ni la Intendencia Municipal del ejemplo anotado podrán transmitir, o retransmitir en su caso, la misma información a empresas privadas.

3º) El ulterior encuadre es el que surge del marco legal aplicable al intercambio de información entre entidades públicas, con arreglo a los arts. 157 y siguientes de la Ley Nº 18.719.

Se trata de otra posibilidad legítima de transmisión o comunicación de datos personales para tratamientos sucesivos a la recolección originaria de los mismos, que no modifica el régimen originario consignado en los arts. 9º y 17 de la Ley Nº 18.331 en tanto rige igualmente la necesidad de recabar el consentimiento del titular de los datos cuando éste es exigible (art. 158 lit. C) de la Ley Nº 18.719).

EN SÍNTESIS

1º) Los datos objeto de consulta son “datos personales” a todos los efectos de la aplicación de la Ley Nº 18.331, normas modificativas y concordantes.

2º) Se trata de datos cuya comunicación a terceros por parte de DI.NA.MA., requieren por regla del previo consentimiento informado de sus titulares, aplicándose a este respecto el art. 10 nal. II) de la Ley Nº 18.381.

3º) El consentimiento no será exigido en aquellas solicitudes de información del tipo consignado en la consulta, cuando resultase aplicable alguna de las excepciones previstas en los arts. 9º y 17 de la Ley Nº 18.331, lo que no resulta posible determinar con criterio general y previo, sino estar al análisis puntual y factual de cada solicitud informativa en concreto.

Firmado:

Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 31, 6 de febrero de 2013.

Se informa consulta relativa a la existencia de mecanismos de control sobre plazos de conservación de los datos de carácter objetivo, así como qué sucede en caso de que existan inscripciones sucesivas en diferentes bases de datos.

INFORME No.		EXPEDIENTE No.
31	2013	2013-2-10-000029

Montevideo, 6 de febrero de 2013

Se realiza informe jurídico en virtud de la consulta formulada por el Sr. Luis Edgardo Olivera, acerca de la existencia de mecanismos de control de los plazos de conservación de los datos de carácter objetivo, así como lo que sucede en caso de que existan inscripciones sucesivas en diferentes bases de datos de este tipo.

I. Introducción

Las bases de datos que brindan información comercial de carácter objetivo, son bases que se nutren con los datos informados por las entidades adheridas a determinadas empresas especializadas en el tema, responsables de las mismas y que brindan ese servicio. Dichas bases también se pueden conformar con datos obtenidos de fuentes de acceso público. La legalidad, respecto a los datos, objeto de recolección y tratamiento, se encuentra regulada en forma explícita en la Ley N° 18.331, art.22.

Esta norma establece que queda “expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia (…), en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor (…).

A su vez, determina que la denominada información comercial u objetiva (cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia), puede registrarse por un plazo de 5 años contados desde su incorporación, y en caso de vencimiento de dicho plazo, cuando la obligación se mantiene incumplida, el acreedor podrá solicitar un nuevo registro por otros 5 años.

En suma, por acreedor se entiende a todo aquel que se encuentra adherido o afiliado a las entidades cuyo giro o negocio consiste en mantener un registro de ese tipo y brindar información de carácter objetivo. Un ejemplo en nuestro país lo constituye Equifax SA (ex Clearing de Informes).

Para brindar este servicio crean y mantienen actualizada una base de datos que debe estar inscripta en el registro que posee la URCDP a tales efectos, y que se nutre con la información

proporcionada por los acreedores adheridos al sistema.
El contenido de la información contenida en estas bases, debe estar únicamente referida a la "solvencia patrimonial o crediticia", de forma tal que se pueda determinar la solvencia económica actual del interesado, por ello es muy importante que se ajusten a los principios de finalidad, proporcionalidad y calidad de la información.
Sobre las preguntas formuladas en la consulta y su análisis

¿Hay algún mecanismo para controlar cuando un acreedor solicita la incorporación en una base de datos, información que ya ha sido expuesta por período de 10 años en otra base de datos?

Por el momento existen sólo dos mecanismos o formas de controlar.

a) Uno de ellos es el que puede realizar el interesado o titular afectado o perjudicado por este tipo de registro, a través del ejercicio de los derechos que se consagran en la Ley. En este sentido hay que considerar que, el art. 14 establece que "todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas".
En cuanto a la posibilidad de ejercer los derechos de rectificación, actualización o supresión por parte del interesado, es oportuno tener presente que el art. 15 de la Ley establece que "toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad (...)".

b) El otro mecanismo de control existente es el que posee la URCDP, como Órgano Regulador que tiene a su cargo la tuición del tratamiento de los datos personales en sentido amplio, incluido el control de lo establecido en el artículo 22 con plena competencia para ello. Toda persona física o jurídica que posea una base de datos de este tipo tiene la obligación de inscribirla en el registro que lleva la URCDP, porque la Ley establece que para que una base de datos se considere legítima es necesario que se encuentre inscripta ante el registro que el órgano de control lleva a estos efectos (art. 28 de la LPDP).
La URCDP realiza el control correspondiente cuando la base se inscribe, contrastando la información que se proporciona con lo establecido en la Ley. También se controla cuando se reciben consultas o denuncias, sobre todo se procede a indagar si la empresa o el particular que es denunciado tiene la base de datos inscripta.
Por otra parte, el Consejo Ejecutivo de la URCDP tiene potestades sancionatorias ante el incumplimiento de la LPDP, pudiendo imponer sanciones de apercibimiento, multa de hasta quinientas mil unidades indexadas y clausura de las bases de datos por un plazo de hasta seis días hábiles (articulo 35 de la LPDP).

¿Qué sucede si el acreedor sucesivamente inscribe al deudor en diferentes períodos, en diferentes bases de datos? ¿No se estaría violando los 10 años que prevé la norma?

El acreedor puede inscribir en diferentes bases al deudor, pero si ello no se ajusta a la realidad o si es incorrecto incurrirá en responsabilidad. El acreedor tiene obligación de controlar la veracidad de los datos y los plazos. También hay que tener presente que sólo tiene derecho a inscribir por una vez más, si pasado el plazo de 5 años inicial, la deuda se mantiene impaga.
Si la veracidad, la calidad de los datos y los plazos no se respetan se estaría vulnerando la Ley y el perjudicado tiene derecho a presentar la denuncia ante la URCDP, así como tiene derecho a ejercer los derechos que la Ley le reconoce en los arts. 14 y 15.
Para evitar que existan registros erróneos, una buena iniciativa está en establecer la obligación a cargo del acreedor de notificar al deudor antes de enviar sus datos a un "clearing" privado, de forma tal que éste pudiera pronunciarse en contra, si los plazos ya se han cumplido o si la información no es correcta.
En este sentido, es importante tener en cuenta que existe actualmente en el Parlamento un Proyecto de Ley presentado por los Senadores Francisco Gallinal y Luis Alberto Lacalle, a efectos de modificar el art. 22.
El art. 1º consagra la obligación de notificar a los deudores personas físicas, la inscripción en registros privados de morosos con acceso a terceros, por parte de acreedores privados y públicos, con requisitos de plazo y contenido al efecto. Se trata de una norma beneficiosa, que le permite al afectado tomar conocimiento de la causa y oportunidad en la que un acreedor resuelve informar la situación a alguna base de datos de titularidad física o jurídica (quedan excluidos los registros públicos).
El art. 3º del proyecto permite prescindir de esta notificación, cuando se está ante obligaciones reconocidas de modo firme en vía judicial o arbitral.

En definitiva, en líneas generales, este proyecto de ley ya ha sido analizado por la URCDP y cuenta con una opinión favorable de la misma.
Las bases de datos alegan no tener los medios para corroborar si los datos a inscribir, ya fueron expuestos por 10 años en otra base de datos, por lo tanto entienden que los 10 años, son tomados desde la incorporación en "su base de datos", sin importar si quien incumplió la obligación, haya o no cumplido 10 años en otra base de datos. ¿No se estaría desvirtuando lo que el legislador quiso decir?
El responsable es quien brinda la información (el acreedor o afiliado al servicio), o sea que es quien debe controlar los plazos y la veracidad de la información. Cuando se cancele una deuda, el acreedor deberá comunicarlo al responsable de la base en un plazo máximo de 5 días hábiles. A su vez, los responsables de la bases de datos tienen un plazo máximo de 3 días hábiles para actualizar la información en su base, una vez que han recibido la comunicación.

Si bien es cierto que éstos últimos, no tienen los mecanismos o la posibilidad de controlar si la información que se le brinda es correcta o no, y si esa deuda ya se encuentra o no en otra base de datos, en cambio sí deben controlar que una vez ingresada la información que se les ha proporcionado, ésta esté en su base de datos actualizada y por el plazo que corresponde. Por otra parte, poseen además otras obligaciones que se vinculan a los demás derechos y principios que se recoge la Ley, a saber:

- deben garantizar los derechos de los titulares de los datos en tiempo y forma (arts. 14 y 15)

- deben utilizar la información de acuerdo con la finalidad para la cual ha sido recolectada (art. 8º) y comunicarlos sólo en aquellos casos que se corresponde con dicha finalidad y limitándose a realizar un tratamiento objetivo de la misma, o sea sin valoraciones personales (art. 22).

- deben mantener la reserva y la seguridad de la información (arts. 10 y 11)

Firmado:
Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 40, de 27 de febrero de 2013.

Se informa consulta realizada sobre datos personales que deben contener las partidas de defunción.

INFORME No.		EXPEDIENTE No.
40	2013	2013-2-10-0000051

Montevideo, 27 de febrero de 2013

I. Introducción

La consulta proviene de la Dirección General de Registro de Estado Civil y refiere al alcance que posee la Ley N° 18.331 respecto a la información contenida en Acta y Certificado de Defunción del Mtro. Julio Castro, emitidos por dicho organismo, los cuales, -a pedido expreso de su familia-, incluyen la causa de la muerte que ha sido determinada por el Equipo de Médicos Forenses, como resultado del "disparo de arma de fuego en contexto de tortura y malos tratos".

La consultante alude a las diferentes normas que se aplicarían a este caso, especialmente a lo establecido en la Ley N° 18.335 de Protección de Derechos de Pacientes y Usuarios de Salud y su Decreto Reglamentario N° 240/010. Se menciona también lo establecido en el Decreto del Presidente de la República de fecha 8 de diciembre de 2011, que reglamenta la implantación del certificado médico de defunción electrónico, respecto a que en el certificado de defunción resumido (el cual es remitido por el Registro de Estado Civil para la inscripción de la defunción), no deberá informarse en forma expresa acerca de los datos clínicos de la causa de la muerte.

Se considera a su vez, que en el marco del decreto antes mencionado, la Dirección General del Registro de Estado Civil dictó una circular (Circular N° 2/2012 de 2 de marzo de 2012), en la que se establece que al labrar el acta de defunción, ya sea en certificado electrónico o en papel, no deberá dejarse constancia de la causa de la muerte si en el certificado no viene indicada, y en caso de que se haya sido indicada, deberá indicarse que consta pero es reservada de acuerdo a la normativa de datos personales.

En el caso del Mtro. Julio Castro, - víctima del terrorismo de Estado y desparecido político desde 1977-, su familiar Hebe Analía Castro Ures, al firmar el Acta de Defunción reitera su voluntad de que en la partida de defunción de su padre aparezca la causa de su muerte (voluntad que ya había manifestado anteriormente según consta en el Folio N° 11 del expediente), tal cual ya figura en el Certificado de Defunción firmado por los integrantes de la Junta Médica que analiza y establece la causa de su muerte. Para ello al firmar la misma agrega que "En este estado, la suscrita Hebe Castro, deja constancia que la causa de la muerte fue disparo de arma de fuego en contexto de tortura. Certificado de defunción N° 172760".

II.- Sobre los fundamentos de la reserva

Se comenzará por analizar los fundamentos legales de la reserva establecidas en el Decreto del Poder Ejecutivo de 8 de diciembre de 2011 sobre Certificado de Defunción Electrónica, recogidos en la Circular N° 2/2012 de la Dirección General de Registro.

En ambos documentos se expresan como fundamentos lo dispuesto en la Ley N° 18.335 sobre Derechos de los Pacientes y Usuarios, su Decreto reglamentario N° 274/010, así como la Ley N° 18.331 de Protección de Datos Personales.

Al respecto es pertinente realizar las siguientes consideraciones:

a) Sobre la primera de las normas mencionadas y su decreto reglamentario cabe observar que de ninguno de los textos normativos surge en forma expresa que la causa de la muerte deba ser considerada, por sí sola, un dato clínico reservado. Ambas reglamentaciones, son normas que claramente mantienen como centro medular de su enfoque, el contenido y el tratamiento de la información que consta en la historia clínica (propiedad del paciente), considerando especialmente que se trata de información reservada que debe ser tratada de acuerdo a lo previsto en el art. 18. En este artículo también se habla de la reserva pero referida a la información contenida en la historia clínica en forma genérica, como conjunto de documentos (art. 18 D).

Conviene considerar además, que la Ley N° 18.335 regula, según lo indica su propio art. 1°, los derechos y obligaciones de los pacientes y usuarios de los servicios de salud con respecto a los trabajadores de la salud y a los servicios de atención de la salud. En el art. 3 se define que se entiende por usuario y que se entiende por paciente.

Sin dudas, lo establecido en este artículo delimita el alcance y el ámbito de aplicación al campo de la salud y refiere a todos los derechos y obligaciones que surgen de la relación existente entre usuarios y pacientes – profesionales y trabajadores de la salud, así como instituciones o prestadores del servicio, tanto públicos como privados.

Por ello cabe preguntarse ¿Por qué aplicar esta norma para fundamentar la reserva de la causa de la muerte del Mtro. Julio Castro en su partida de defunción? Es claro que el caso no refiere a los derechos de un paciente ni de usuario del sistema de salud. Estamos hablando de una persona que fue víctima de terrorismo de Estado y mantuvo un estatus de desaparecido político hasta que sus restos fueron encontrados y la causa de su muerte fue dictaminada por un Equipo Forense especialmente conformado para ello.

Por ende, el contexto del caso determina que se trate de una situación muy diferente a la que aborda la Ley N° 18.335. Coincidimos plenamente con la asesora jurídica que formula esta consulta: este contexto hace que toda información que ilustre sobre el carácter de víctima de la violencia del Estado que sin dudas posee el Mtro Julio Castro, adquiera un valor testimonial que trasciende el carácter de mero dato clínico personal.

b) En cuanto al fundamento que alude en forma genérica a la normativa de datos

personales, cabe considerar que si bien la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, establece a la reserva como uno de los principios que deben estructurar la protección de datos personales, sin embargo también establece excepciones que deben ser debidamente armonizadas con los demás derechos que se contraponen en cada caso concreto.

Por ejemplo, el art. 17 indica que los datos personales objeto de tratamiento podrán ser comunicados sin previo consentimiento cuando así lo disponga una ley de interés general o en los supuestos del art. 9°. En cuanto a que así lo disponga una Ley de interés general, deberían considerarse especialmente la Ley N° 18.381 de Acceso a la Información Pública y la Ley N° 18.596 de Actuación ilegitima entre el 13 de junio de 1968 y el 28 de febrero de 1985 y Reconocimiento y Reparación a las Victimas, además de la normativa de derecho internacional de los DD.HH que nuestro país a ratificado y que garantiza derechos a las víctimas de terrorismo de Estado. Sobre las dos normas antes mencionadas nos referiremos con especial detenimiento más adelante.

El art. 17 señala además que no será necesario el consentimiento cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación. Por su parte, en la modificación introducida por el art. 43 de la Ley N° 18.996 de 7 de noviembre de 2012 (Ley de Rendición de Cuentas y Balance Presupuestal del 2011), se consideran como fuentes públicas o accesibles al público, entre otras, a las publicaciones oficiales y las publicaciones en medios masivos de comunicación, en cualquier soporte, así como a todo registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos, puedan ser consultados, difundidos o utilizados por parte de terceros.

En este caso, la causa de la muerte es un dato que ha sido publicado en diversos medios de información, así como ya es parte de libros o informes oficiales que tienen circulación pública y masiva. Por ejemplo, en el comunicado de la Suprema Corte de Justicia[1], o en la Wikipedia[2], en diversos artículos del Diario El País[3], o en el Libro “En cuanto venga Julio” del periodista Pablo Manuel Méndez (2012), entre innumerables testimonios escritos, libros, artículos, etc. de circulación nacional e internacional.

Por otra parte, en un caso tan especial como el que estamos analizando, también corresponde analizar el rol o papel que juega el Interés General, concepto que permite afirmar que la información que se pretende reservar, es de interés público y debe circular libremente, dado s carácter testimonial.

Entonces ¿Porqué mantener en reserva un dato que ya es público y que además está inserto en el contexto de un caso donde además existe un evidente interés general en que esa información sea difundida y accedida por todos?

---

1 http://www.subrayado.com.uy/Resouces/Uploads/RelatedFiles/Docs/castro_poder_judicial.pdf

2 http://es.wikipedia.org/wiki/Julio_Castro

3 http://historico.elpais.co.uy/111202/pnacio-610088/nacional/julio-castro-fue-ejecutado-de-un-disparo, http:// histórico.elpais.com.uy/12/03/06/ultimo_628908.asp.

c) Por último, es necesario considerar la existencia de la Ley N° 18.381 de Acceso a la Información Pública de 17 de octubre de 2008, que en el art. 2° establece que se considera información pública toda la que emane o esté en posesión de cualquier organismo público, sea o no estatal, salvo las excepciones o secretos establecidos por ley, así como las informaciones reservadas o confidenciales.

Esta norma debe ser considerada en el balance de derechos que corresponde realizar en los casos como el que nos ocupa. Tal como señala, el Dr. Piñar Mañas los actuales sistemas democráticos deben articularse en torno a tres pilares fundamentales "protección de datos, seguridad y transparencia"[4].

La Ley de Acceso a la Información Pública además, debió ser considerada a la hora de reglamentar acerca de que el dato clínico de la muerte de una persona debe ser reservada en todos los casos, entre otras cosas porque el art. 8 de la misma establece el carácter que deben tener las excepciones al acceso a la información pública, entre las que cabe resaltar que las mismas deben ser de interpretación estricta y establecidas por ley. Esto último es importante porque la doctrina mayoritaria en esta materia, así como la propia Corte Interamericana de DD.HH, entienden que debe ser establecidas por ley en sentido foral, o sea no se puede establecer una excepción al acceso a la información pública mediante decreto.

Por otra parte, la información reservada es regulada en el art. 9º de la Ley Nº 18.381, donde se describen las situaciones o hipótesis donde se habilita legalmente a que una información sea reservada por parte de un organismo, en forma fundada y por determinado período de tiempo (15 años). Por otra parte, se considera que la información confidencial es la establecida en el art. 10 de la misma Ley, entre la cal encontramos los datos personales que requieran previo consentimiento informado (art. 10 Num.II).

En conclusión, si el dato de la causa de la muerte fuera información reservada debería desclasificarse a los 15 años, por ende debería haber sido clasificado como información reservada de acuerdo a los arts. 9 y 11 de la Ley Nº 18.331, en cambio si es un dato personal que requiere previo consentimiento informado (como creemos que podría llegar a ser en ciertos casos, como por ejemplo muerte a causa de una enfermedad estigmatizante) debería ser considerada información confidencial, sin estar sujeta a plazo de desclasificación, lo cual es más coherente tanto con el tipo de información de que se trata como con el tipo de documento en que se inserta el dato (partida de defunción).

Por último, en el caso concreto corresponde que se considere además el art. 12 de la Ley Nº 18.381, donde se expresa que las excepciones al derecho de acceso a la información pública se consideran inoponibles en aquellos casos donde la información solicitada por un tercero esté relacionada a las violaciones de los derechos humanos.

En este caso, tal como señalan autores como Víctor Abramovich y Christian Courtis, se trata de

4 PIÑAR MAÑAS, José. "Seguridad, Transparencia y Protección de Datos: el futuro de un necesario e incierto equilibrio". Documento de trabajo 147/2009. Fundación Alternativas. http://www.faltenativas.org/documentos (20 de abril de 2010).

otra forma de entender el derecho a la información, “no como un fin en sí mismo, sino como un instrumento de concreción de otros derechos, valores o principios”[5]. Este fundamento sostiene la idea que la causa de la muerte de esta persona, no se trata de un mero dato personal sino que trasciende este concepto y adquiere un valor testimonial, que se debe relacionar con el derecho a la información pública y a la libertad de expresión que posee la sociedad en su conjunto, así como a los derechos que poseen las víctimas de terrorismo de Estado y sus familiares, en el marco del concepto de reparación integral que debe implementar el Estado hacia ellos.

Nuestro país a través de la Ley Nº 18.596 de Actuación Ilegítima del Estado entre el 13 de junio de 1968 y el 28 de febrero de 1985 y Reconocimiento y Reparación a las Victimas de 18 de setiembre de 2009, no solo ha dispuesto que se debe reparar a las víctimas de terrorismo de Estado y a sus familiares, sino que en el art. 7º establece expresamente que “El Estado promoverá acciones materiales o simbólicas de reparación moral con el fin de restablecer la dignidad de las víctimas y establecer la responsabilidad del mismo. Las mismas tenderán a honrar la memoria histórica de las víctimas del terrorismo y del uso ilegítimo del poder del Estado…”

III. Conclusiones finales

a) En el caso, desde el punto de vista de la normativa de protección de datos personales, la Dirección General de Registro se encuentra habilitada para que la causa de la muerte figure en el Acta y en la Partida de Defunción del Mtro. Julio Castro, tal cual lo solicita y consiente expresamente su familia.

b) Además resulta plenamente aplicable lo dispuesto en el art. 17 de la Ley N° 18.331 que indica que los datos personales objeto de tratamiento podrán ser comunicados sin previo consentimiento cuando así lo disponga una ley de interés general, ya que existen normas específicas en nuestro ordenamiento interno que habilitan la comunicación de esta información (Ley N° 18.381 y Ley Nº18.596), además de otros instrumentos de Derecho Internacional (Convenciones y Tratados) que garantizan el derecho de acceso a la información pública y a la verdad, que nuestro país ha ratificado.

c) Por otra parte, corresponde además la aplicación de la modificación hecha por la Ley N° 18.996, considerando en definitiva que se trata de un dato que no requiere el consentimiento previo para su comunicación a terceros, ya que figura en diversas fuentes públicas o accesibles al público, y además debe ser público todo registro o publicación en el que prevalezca el interés general en cuanto a que los datos personales en ellos contenidos puedan ser consultados, difundidos o utilizados por parte de terceros.

Firmado:

Dra. Graciela Romero

Derechos Ciudadanos

5 Víctor Abramovich & Christian Courtis, El acceso a la información como derecho, 1 ANUARIO DE DERECHO A LA COMUNICACIÓN, vol. 1, 2000 2.2-2.2.4

Informe N° 47, de 5 de marzo de 2013.

Se informa consulta respecto al alcance del artículo 9º de la Ley Nº 18.331.

INFORME No.		EXPEDIENTE No.
47	2013	2011-2-10-0000602

Montevideo, 5 de marzo de 2013

I. Introducción

El Ministerio de Educación y Cultura recibe una solicitud de acceso a la información pública en el marco de la Ley N° 18.381. En la misma se solicita acceder al domicilio y al teléfono particular del titular de dicha institución.

La consulta remitida por este Ministerio a la URCDP refiere a que, conforme lo establecido por el art. 10 Lit. II de la Ley N° 18.381, los datos solicitados se encuentran comprendidos dentro de los categorizados como información confidencial, por lo que requieren el previo consentimiento informado para ser comunicados. Agregan que sin embargo, el art. 9º lits. B) y C) de la Ley N° 18.331 establece excepciones donde no será necesario el consentimiento informado del titular, ya sea cuando es para cumplir con las funciones propias de los poderes del Estado o cuando se trate de listados que en caso de personas físicas, se limiten a nombre y apellidos, documento de Identidad, nacionalidad, domicilio y fecha de nacimiento.

En base a ello, el domicilio se encontraría incluido en este listado no así el teléfono móvil.

II. Sobre el balance y la ponderación de los derechos

En este caso corresponde realizar un análisis y ponderación de los derechos e intereses en juego (en este caso acceso a la Información pública y protección de datos personales) a la luz de los diferentes principios que guían o estructuran la Ley N° 18.331, sobre todo los principios de consentimiento, finalidad y proporcionalidad.

Indefectiblemente debe existir un juicio de proporcionalidad basado en la idoneidad, la necesidad de los datos y el equilibrio de derechos. Esto significa a su vez, que debe existir una justificación que resista ese juicio y muestre como imprescindible la utilización de esa información, por ejemplo para investigar un delito, para mejorar la transparencia de la administración, evitar un peligro inminente o contribuir a una investigación judicial o administrativa.

Corresponde tener presente que aún, respecto a aquellos datos que no requieren previo consentimiento informado, las Entidades Públicas también deberán observar los principios que estructuran la Ley N° 18.331. En este sentido, esto es lo expresado en los comentarios realizados por el Grupo del Artículo 29 (G29), en la consulta realizada en el marco del proceso de adecuación de Uruguay a la Unión Europea.

A su vez, el art. 7° de la Ley N° 18.331 contempla la necesidad de que el tratamiento y/o comunicación de un determinado dato personal, deba ser proporcional a la finalidad que lo motiva.

En resumen corresponde considerar cual es la finalidad implícita al brindar el acceso o publicidad a determinado tipo de dato personal, la cual deberá estar en consonancia con lo establecido en la Ley N° 18.331, art. 8°, que establece que los datos objeto de tratamiento no podrán utilizarse para finalidades distintas o incompatibles a aquellas que motivaron su obtención.

¿Cuál es la finalidad de acceder al domicilio y al teléfono particular del jerarca de un Ministerio? Creemos que la misma, -armonizando con lo establecido en la Ley N° 18.381-, no podría ser otra que la de controlar la gestión y el correcto funcionamiento del Ministerio, incluso formular una petición, realizar una denuncia, etc. para alcanzar algunos de estos fines, no sería necesario pero sí desproporcionado brindar acceso a este tipo de información personal del Ministro, porque en definitiva, el acceso debe versar sobre los datos relacionados con el cargo y función que cumplen los funcionarios, en concordancia con lo establecido en el art. 38.8 del Decreto N° 232 reglamentario de la ley N° 18.381.

Por otra parte, no creemos de aplicación a este caso lo establecido en el art. 9° B) de la Ley N° 18.331, que establece que no será necesario el previo consentimiento cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

Esta situación abarca a la recolección de datos, es decir cuando los datos son recolectados por parte de un organismo (datos de sus funcionarios, proveedores, ciudadanos, interesados, administrados, etc.), para poder cumplir con sus funciones, o cuando esta recolección se encuentra habilitada por una ley. Por ejemplo, el MEC puede recolectar determinados datos de aquellos interesados que se presenten a realizar trámites ante sus oficinas, sin obtener su consentimiento previo y por escrito, si esos datos son los necesarios para terminar el trámite o cumplir con su función.

III.- Conclusiones finales

Tal como se establece por parte de la Red Iberoamericana de Protección de Datos, si se solicita la publicidad o el acceso a determinados datos personales de los funcionarios públicos que requieren previo consentimiento informado, deberá realizarse la Prueba de Interés Público, considerando especialmente:

- si existen excepciones en favor de la publicidad de dichos supuestos en las leyes respectivas,

si con la divulgación de los datos personales se puede vincular o conocer el correcto desempeño de las responsabilidades o tareas asignadas al funcionario en un caso concreto,

- si dichos datos son considerados como información propia del individuo, no de su puesto en la estructura laboral, y

- si la divulgación añade información necesaria para la rendición de cuentas o la transparencia en el uso de recursos públicos[6].

Firmado:

Dra. Graciela Romero
Derechos Ciudadanos

6 Ver Documento de la Red Iberoamericana de Protección de Datos. EL ACCESO A LA INFORMACIÒN PÚBLICA Y LA PROTECCION DE LOS DATOS PERSONALES Huixquilucan (Estado de México), 4 de noviembre de 2005.

Informe N° 49, de 12 de marzo de 2013.

Se informa consulta sobre la inclusión en la nueva versión del certificado de defunción, impreso y electrónico, del número de teléfono celular y del correo electrónico del médico certificador.

INFORME No.		EXPEDIENTE No.
49	2013	2013-2-10-0000080

Montevideo, 12 de Marzo de 2013

I. Antecedentes

1. La Unidad de Información Nacional de Salud (en adelante UINS), consulta sobre la pertinencia de incluir en la nueva versión del Certificado de Defunción impreso y electrónico, el número de teléfono celular y/o correo electrónico del médico certificador, sin violentar o contradecir los principios de la Ley Nº 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data.

2. Motiva la consulta, la necesidad de contacto de la UINS con el médico certificador, para esclarecer o completar datos ilegibles o faltantes del Certificado de Defunción, debido a que el 33% llega al Ministerio de Salud Pública con incoherencias o falta de datos, situación que afecta la calidad de las Estadísticas Vitales.

3. Corresponde a la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) evacuar la consulta, en mérito al cometido de asistencia y asesoramiento, que le fuera atribuido por el art. 34 lit. A) de la Ley N° 18.331.

II. Análisis

A.Generalidades

4. Certificado de Defunción Electrónico.- El decreto N° 249/007 de 9 de Julio de 2007, implanta el Certificado de Defunción electrónico “en base a la utilización y extensión de la red informática requerida para el Certificado de Nacimiento”, en reconocimiento de la necesidad de mejorar los sistemas de identificación de personas físicas en el Uruguay utilizando herramientas informáticas, y en el entendido que la identificación de las personas físicas en el país se basa en el Certificado de Nacimiento, la inscripción en el Registro de Estado Civil, la Cédula de Identidad y el Certificado de Defunción.

Por su parte, el decreto N° 431/011 de 3 de Enero de 2012, aprueba el modelo de Certificado de Defunción y de Certificado de Defunción Resumido en formato electrónico, indicando los contenidos de cada uno en el caso de los datos del fallecido, no así del médico certificador cuyos datos a mencionar no se regulan.

B. Inclusión de Datos

5. Dato personal.- El teléfono fijo o celular, así como el correo electrónico del médico certificador son datos personales, de acuerdo a las previsiones del art. 4º lit. D) de la Ley N° 18.331.

6. Comunicación de datos.- La inclusión del teléfono fijo o celular, y/o el correo electrónico del médico certificador en el Certificado de Defunción electrónico, se enmarca en la definición legal de comunicación de datos personales dada por la Ley N° 18.331. La cual, en principio, deberá contar con el previo consentimiento informado de sus titulares.

Según lo dispuesto por el art. 4º lit. B) de la Ley N° 18.331, estaremos ante una comunicación de datos toda vez que exista "revelación de datos realizada a una persona distinta del titular de datos". Por su parte, el art. 17 de la citada norma, exige que la comunicación se realice "para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo", salvo las excepciones al previo consentimiento taxativamente dispuestas en el mismo artículo.

Corresponde por tanto revisar, si la comunicación que nos ocupa se enmarca dentro de alguna de las excepciones previstas para poder comunicar datos personales sin consentimiento de sus titulares, en el entendido que aun así, subsistirá el requisito del interés legítimo.

6.1 Excepciones.- Del elenco tasado de excepciones, aplica la remisión al art. 9º lit. B) y D).

6.1.1 Artículo 9 literal B).- Dispone que no será necesario el previo consentimiento informado cuando "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". No cabe duda, que velar por la salud de los habitantes de la República, es una función propia del Estado, así como una obligación legal.

En efecto. Según lo dispuesto por el art. 44 de la Constitución de la República "El Estado legislará en todas las cuestiones relacionadas con la salud e higiene públicas, procurando el perfeccionamiento físico, moral y social de todos los habitantes del país".

Por su parte, la Ley Orgánica del Ministerio de Salud Pública[7], dispone que "Compete al Poder Ejecutivo por intermedio de su Ministerio de Salud Pública, la organización y dirección de los servicios de Asistencia e higiene". Siendo dicho Ministerio la policía de la Medicina y de las profesiones derivadas[8]. Contralor, que en materia deontológica es ejercido por el Colegio Médico del Uruguay[9].

6.1.2 Artículo 9º literal D).- Establece que no será necesario el previo consentimiento cuando los datos "deriven de una relación contractual, científica o profesional

7 Art. 1º de la Ley N° 9.202, de 12 de enero de 1934.

8 Arts. 2º nal. 6º y 13 de la Ley N° 9.202, de 12 de enero de 1934.

9 Art. 1º de la Ley N° 18.591, de 18 de setiembre de 2009.

del titular de los datos, y sean necesarios para su desarrollo o cumplimiento".
Necesariamente, entre el cuerpo médico y el Ministerio de Salud Pública existe una relación científica y profesional, debido al trato y comunicación relativos a la profesión desempeñada, la que además puede ser contractual, cuando se trate de médicos empleados en nosocomios públicos.
De lo precedentemente expuesto, se desprende, que la inclusión de los datos teléfono fijo o celular, y/o correo de electrónico del médico certificador, se encuentran excluidos del requisito del previo consentimiento informado en el caso del Certificado de Defunción.
En cuanto al interés legítimo exigido por el art. 17 de la Ley N° 18.331 para que proceda la comunicación, entiendo que en la especie, encuentra fundamento en el cuidado de la Salud en cuanto bien supremo.

7. Inteligibilidad.- El ordenamiento jurídico debe ser visto como un todo y sus normas interpretarse en contexto. En este sentido, si bien excede las previsiones de la Ley de Protección de Datos Personales y la competencia de la Unidad, corresponde recordar, que la Historia Clínica constituye un conjunto de documentos en los que figura la evolución del estado de salud de una persona desde el nacimiento hasta la muerte. Su correcto llenado forma parte de la atención a la salud, siendo responsabilidad del trabajador actuante la realización del registro correspondiente de manera completa, ordenada, veraz e inteligible[10].
Por tanto, el Certificado de Defunción integra la Historia Clínica y su llenado completo e inteligible por parte del médico certificador, constituye una obligación a ser cumplida.

III. Conclusiones

1. El presente informe refiere a la pertinencia de incluir en la nueva versión del Certificado de Defunción impreso y electrónico, el número de teléfono fijo o celular, y/o correo electrónico del médico certificador, de cara a la normativa de Protección de Datos, sin considerar la forma o procedimiento que correspondería seguir al respecto.

2. La inclusión en el Certificado de Defunción de los datos teléfono fijo o celular, y correo electrónico del médico certificador, no encuentra impedimento en la Ley N° 18.331.

3. Se trata de una comunicación de datos excepcionada del requisito del previo consentimiento informado de su titular, conforme lo dispuesto en los lits. B) y D) del art. 9º de la citada norma, siendo el interés legítimo el cuidado de la Salud en cuanto bien supremo.

4. Corresponde recordar, de acuerdo con la normativa nacional vigente, que el Certificado de Defunción forma parte de la Historia Clínica, y que su llenado completo e inteligible por parte del médico certificador, es una obligación que debe ser cumplida.
Es todo cuanto tengo que informar.

Firmado:
Dra. Bárbara Muracciole
Derechos Ciudadanos

10 Arts. 18 lits. D) y 19 de la Ley N° 18.335 de Derechos y Obligaciones de los Pacientes y Usuarios de los Servicios de Salud, de 15 de Agosto de 2008 y 29 del Decreto reglamentario N° 274/010 de 8 de Setiembre de 2010.

Informe Nº 54, de 13 de marzo de 2013.

Se informa consulta respecto a si se pueden realizar determinadas comunicaciones de datos a efectos de facilitar el otorgamiento y control del beneficio de la Asignación Familiar.

INFORME No.		EXPEDIENTE No.
54	2013	2013-2-10-0000096

Montevideo, 13 de marzo de 2013

La consulta refiere al tratamiento de datos personales de escolares y liceales, más concretamente a la legalidad de solicitar la comunicación de ciertos datos personales de escolares y liceales a las Instituciones de Enseñanza Privada, dentro del marco del régimen que regula el beneficio de Asignación Familiar, siendo promotores conjuntos de la consulta el Banco de Previsión Social, el Ministerio de Educación y Cultura, y las Asociaciones que vinculan a las mencionadas Instituciones de Enseñanza Privada.
Se exponen necesidades de buena administración vinculadas con el otorgamiento y mantenimiento de la Asignación Familiar en favor de sus beneficiarios, todo ello dentro del marco de las leyes Nº 15.084 y Nº 18.227.
Se consulta si resulta adecuado al régimen de protección de datos personales, requerirle a dichas Instituciones las siguientes categorías de datos en formato electrónico:

- Cédula de Identidad.
- Nombre completo.
- Fecha de nacimiento.
- Fecha de matriculación.
- Indicador de permanencia en los estudios, o asistencia regular, o progreso educativo, que justifica ser acreedor de la prestación mencionada.
- Indicador de recibo o postulación a recibir el beneficio.

Se fundamenta el requerimiento en la necesidad de contar con las mejores posibilidades de cruzar la información así obtenida con la que ya dispone el Banco, facilitando la operativa y control en el otorgamiento de la prestación en juego a lo largo del tiempo, acorde a los requisitos legales y reglamentarios.
Se argumenta que, en caso de no poder contar con la información por la vía propuesta, se debería convocar personalmente a los implicados uno a uno, lo que demandaría esfuerzos y molestias a evitarse aplicando el medio electrónico a una información que ya existe.
A juicio del suscrito Asesor, del punto de vista del derecho a la protección de los datos personales, la comunicación propuesta es compatible con lo dispuesto por la Ley Nº 18.331,

en tanto y cuanto se limite a los casos de aquellas familias que perciben el beneficio.
En tal sentido se considera que dicha solicitud no ofrece reparos jurídicos atendiendo a los siguientes fundamentos:

1º- Se trata de una actividad que no va contra los DD.HH. ni es contraria a las leyes o la moral públicas (art. 6º de la Ley), por el contrario reafirma todos estos valores al servir a la comprobación objetiva de algunos de los requisitos esenciales para la generación o mantenimiento de un derecho sujeto a contralor; requisitos que, a su vez, tienen previsión legal y reglamentaria (los arts. 5º y 8º de la Ley Nº 15.084, y 12 del Decreto 227/981 son los más pertinentes al caso).

2º- Cumple con las notas de adecuación, ecuanimidad y no excesividad previstas dentro del "principio de veracidad" que prevé la Ley (art. 7º de la Ley). Si en el futuro se quisiera ampliar la tipología de datos a comunicar, cabría recibir una nueva consulta al respecto.

3º- Cumple con el "principio de finalidad" (art. 8º de la Ley) en la medida que se trata de un uso declarado y lícito de la información a obtener, marco a respetar por el consultante acorde a sus propias expresiones, en cuanto al destino que se dará a estos datos.

4º- Siempre referido al "principio de finalidad", el destino de los datos obtenidos que plantea la consulta resulta admisible y armónico, tanto por lo que refiere al respeto del derecho a la protección de datos personales, como por favorecer el cumplimiento de otros derechos y acciones positivas que se enmarcan dentro de las políticas y normas sobre gobierno electrónico vigentes en el país.

5º- No requiere consentimiento de los titulares por aplicación de las excepciones previstas en los arts. 9º B, 9ºC y 17 B de la Ley.

EN CONCLUSIÓN:

La solicitud de comunicación planteada es considerada lícita, y no precisa del consentimiento de los titulares de los datos ni sus representantes legales, con la salvedad de que debe limitarse a las personas y grupos familiares que son atributarios del beneficio de Asignación Familiar.
Se sugiere recomendar que la solicitud de comunicación se lleve a cabo cumpliendo en todo momento con los principios y obligaciones, legales y reglamentarios en vigencia sobre la protección de datos personales.
En especial, y entre otros deberes, se tendrán presentes el criterio ya expuesto por el propio consultante de limitar la colecta a lo estrictamente necesario para el cumplimiento de la finalidad perseguida, la eliminación de los datos recibidos una vez cumplida las finalidades en juego, y el aseguramiento del derecho de acceso de los titulares o sus representantes legales para poder conocer y eventualmente rectificar informaciones erróneas o desactualizadas.

Firmado:
Dr. Marcelo Bauzá
Derechos Ciudadanos

Informe N° 84, de 29 de abril de 2013.

Se informa consulta relativa a la pertinencia de la publicación de determinados datos personales en un sitio web con carácter de dato abierto.

INFORME No.		EXPEDIENTE No.
84	2013	2011-2-10-0000130

Montevideo, de 29 de abril de 2013

I. Antecedentes

La Intendencia de Montevideo consulta acerca de la posibilidad de publicar en la web institucional el índice de archivo del Servicio de Registro de Estado Civil, con carácter de "dato abierto".

Consideran que los datos a los que podría accederse con esta publicación, no son datos que requieren previo consentimiento informado, y serían los siguientes: nombre completo de la persona y su fecha de nacimiento, matrimonio o defunción, con referencia al Año, Sección y Número de Acta, sin asociar la imagen de la partida de que se trate.

II. Análisis y marco jurídico de aplicación

Respecto al carácter de "dato abierto", corresponde mencionar que el criterio aplicado por la IM, -y plenamente compartido-, siempre ha consistido en asegurarse que los datos que publica con este carácter sean efectivamente públicos, en definitiva que no se trate de información reservada, confidencial o secreta, según lo establecido en la Ley N° 18.381 de Acceso a la Información Pública y en la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data.

En la Resolución N° 640/010 de la IM se establece que debe brindarse el acceso libre a los datos, cuando se cumplan una serie de condiciones, entre las cuales se menciona que todos los datos no estén sujetos a limitaciones de privacidad, seguridad o privilegios.

Creemos que en este sentido, cuando dichos datos se publiquen en forma nominada y no en forma anónima o disociada, perderían ya el carácter de "dato abierto", para pasar a ser datos personales.

En nuestro país, de acuerdo con lo establecido en la Ley N° 18.331, cualquier iniciativa de datos abiertos debe considerar el anonimato de personas tanto físicas como jurídicas, pues el art. 4° de esta Ley establece que dato personal se trata de información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables. Con la amplitud que ello implica, tampoco cabría la posibilidad de abrir datos, que sumados entre sí o relacionados de tal forma, permitan identificar a una persona física o jurídica, porque la Ley dice "determinables", o sea que identifiquen o permitan identificar si se asocian de determinada forma.

En el art. 9º lit. C) de esta norma se indica que “El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse”. Agrega que: “No será necesario el previo consentimiento cuando: C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento”. Como vemos algunos de los datos que se van a publicar no están incluidos en este listado.

A su vez, esta norma se estructura en base a una serie de principios, que delimitan la responsabilidad de quienes poseen y/o realizan tratamiento de datos personales. Estos principios cumplen la función de guiar la interpretación y la resolución de todas las cuestiones que puedan suscitarse en la aplicación de sus disposiciones (art. 5° in fine).

Entre ellos se encuentra el de finalidad (art. 8°), que establece que los datos objeto de tratamiento, no podrán ser utilizados para finalidades distintas o incompatibles a aquellas que motivaron su obtención. En este caso, los datos se han obtenido, por parte del Registro Civil, para determinada finalidad que hace a la conformación de la identidad y del estado civil de los administrados. Para cumplir con esta finalidad no es necesario que los datos se publiquen en la web.

Recordemos que la Dirección General del Registro del Estado Civil y las Intendencias Departamentales tienen la función de conservación, custodia, ordenado e indizado de los documentos que prueban el estado civil de las personas. Estos documentos refieren tanto a hechos jurídicos o sea eventos cuyos efectos no resultan de la voluntad humana (nacimientos y defunciones), como a actos jurídicos o sea manifestaciones de voluntad dirigidas a producir determinados efectos (matrimonio, reconocimiento de la paternidad natural, el repudio de dicha paternidad, legitimación de hijos naturales por matrimonio, etc.), como a sentencias o resoluciones judiciales (divorcio, nulidad de matrimonio, etc.).

En definitiva, la función del Registro de Estado Civil es anotar los hechos o actos que atañen al estado civil, con la intervención de un funcionario público competente (Oficial del Estado Civil) en los libros correspondientes y con las formalidades que la ley prescribe.

El art. 17 de la Ley N° 18.331 por su parte indica que, la comunicación de datos personales objeto de tratamiento, sólo podrá realizarse para cumplir con los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, salvo que así lo disponga una ley de interés general o en los dispuestos del art. 9° (por ejemplo los listados), o los datos sean disociados de sus titulares (anonimizados).

A su vez, el art. 7° contempla la necesidad de que el tratamiento y/o comunicación de un determinado dato personal deba ser proporcional a la finalidad que lo motiva. En el caso, la comunicación de ciertos datos o su publicación, como lo son el dato sobre el matrimonio o la defunción de una persona, a nuestro juicio resultaría excesiva y desproporcionada de acuerdo con la finalidad del registro.

III. Conclusiones

La publicidad de determinados datos personales, como los datos de matrimonio o de defunción, sin el consentimiento del titular, vulneran las disposiciones de la Ley N° 18.331.

En este sentido, debe considerarse que dicho tratamiento debe ajustarse a los principios de proporcionalidad (art. 7°) y de finalidad (art. 8°), así como a lo establecido en los arts. 9° y 17 A) de la misma norma.

En definitiva, el índice debería publicarse sin los datos antes indicados o en forma anónima, o sea sin identificar a los titulares de los mismos (art. 17 D).

Firmado:

Dra. Graciela Romero
Derechos Ciudadanos

Informe Nº 92, de 6 de mayo de 2013.

Se informa consulta acerca de la legalidad de exigir la inclusión del diagnóstico en los certificados médicos que justifican ausencias por enfermedad.

INFORME No.		EXPEDIENTE No.
92	2013	2011-2-10-0000159

Montevideo, 6 de mayo de 2013

I. Antecedentes

1. Oscar Gabriel Juanvelz Romero, consulta sobre la legalidad de exigir la inclusión del diagnóstico en los certificados médicos que justifican ausencias por enfermedad, de cara a las disposiciones de la Ley Nº 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data.

2. Corresponde a la Unidad Reguladora y de Control de Datos Personales evacuar la consulta, en mérito al cometido de asistencia y asesoramiento, que le fuera atribuido por el artículo 34 literal A) de la citada norma.

II. Análisis

A.Generalidades

3. Certificado médico.- Desde la óptica médico-legal, certificado viene de certificatio, cierto, seguro, indudable. Es un testimonio escrito referente a un hecho clínico. El profesional médico después de haberlo comprobado personalmente lo extiende a pedido de un paciente o de los familiares del mismo[11].

Del punto de vista jurídico, Eduardo J. Couture nos enseña, que es la: “Atestación que un experto hace de un hecho que le consta en razón del ejercicio de su profesión”.

Ambas acepciones resultan coincidentes: se trata de acreditar una circunstancia o hecho, que debe haber realmente sucedido.

Inclusión de diagnóstico

Al tratar la inclusión del diagnóstico en un certificado médico, necesariamente abordamos dos temas centrales sobre los cuales se sustenta la relación médico-paciente. Ellos son: el secreto médico profesional y el tratamiento de los datos sensibles, su comunicación en la especie.

4. Secreto Médico Profesional.- “El secreto médico, como no podía ser de otra manera, forma parte del secreto profesional y su existencia proviene del mismo Juramento Hipocrático (“De aquello que vea u oiga en el ejercicio o aún fuera del ejercicio de mi profesión, silenciar lo que jamás deba divulgarse, observando la discreción como un deber para semejantes casos”). Y desde aquellos tiempos hasta los nuestros, es obviamente reconocido como un deber ético

11 *Dr. Guido Berro Rovira, Jornadas sobre Certificaciones y Constancias Médicas pág. 8 y 9, SMU, 2002.*

del médico y un derecho del paciente"[12].

Se encuentra regulado en el art. 302 del Código Penal que reza: "(Revelación de secreto profesional) El que, sin justa causa, revelare secretos que hubieran llegado a su conocimiento, en virtud de su profesión, empleo o comisión, será castigado, cuando el hecho causare perjuicio, con 100 U.R. (cien unidades reajustables) a 600 U.R. (seiscientas unidades reajustables) de multa".

Estamos ante un secreto que opera de pleno derecho, sin necesidad que el paciente lo solicite, lo que significa que desde el inicio, el médico está llamado a guardar silencio sobre lo que el paciente le confíe y él mismo conozca, aún accidentalmente. Se trata de un secreto que no puede ser revelado ni siquiera por orden de la Justicia Penal. En este sentido son claras las disposiciones del art. 220 nal 3º del Código del Proceso Penal, al decir que: "Deberán abstenerse de declarar sobre los hechos secretos que llegasen a su conocimiento en razón del propio estado, oficio o profesión, bajo pena de nulidad" (...) "Los médicos, farmacéuticos, obstetras y demás técnicos auxiliares de la ciencia médica".

Su relevamiento, por ende, únicamente podrá deberse a justa causa, obligación legal o autorización expresa y escrita del paciente.

Toda la relación médico-paciente, está comprendida en el secreto médico. Podemos decir que "Integran el secreto profesional del médico la naturaleza de la enfermedad, la comunicación del pronóstico, que solo puede hacerse al interesado o a personas inmediatas y justamente interesadas en el paciente, salvo determinadas excepciones que veremos, así como todas las circunstancias de hecho que rodeen a la enfermedad"[13]. No existe duda en cuanto a que el diagnóstico, forma parte de esta relación, y por ende se encuentra alcanzado por el secreto médico profesional, por lo que solicitarle al médico su revelación, en este caso consignándolo en el certificado médico, sin consentimiento del paciente, es pedirle que cometa un delito.

e. Datos sensibles. Comunicación- La inclusión del diagnóstico del paciente en el certificado médico, se enmarca en la definición legal de comunicación de datos personales dada por la Ley N° 18.331[14], desde que estamos ante una revelación de datos realizada a una persona distinta del titular, puesto que dicho documento tiene como destinatario al empleador. Tratándose de datos sensibles[15], especialmente protegidos, deberá contar con el previo consentimiento informado y escrito de sus titulares, ya que "ninguna persona puede ser obligada a proporcionar datos sensibles. Estos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular"[16], salvo excepciones tasadas, que no aplican en este caso.

---

12 Adriasola, Gabriel, "Alcances del Secreto Profesional del Médico", pág. 1. Disponible en https://docs.google.com/file/d/0B1-UD3Javk_VWXRhdWgtamVwOTg/edit?usp=drive_web&pli=1*, visita realizada el 6 de Mayo de 2013.*

13 Op. cit.

14 Artículo 4 literal B).

15 Artículo 4 literal E).

16 Artículo 18 inciso primero.

Por tanto, desde el punto de vista del paciente, el diagnóstico es información sensible que requiere su consentimiento escrito para ser revelado a terceros, en la consulta que tratamos: el empleador.

5. Sistema Nacional de Certificación Laboral.- El Banco de Previsión Social instauró el Sistema Nacional de Certificación Laboral[17], a partir del cual, el médico certificador debe llenar un formulario en dos vías en el cual se indican los datos identificatorios del paciente y la patología, entre otros. Una vía se entrega al usuario y otra a la IAMC empleadora del médico certificador. Una vez que la IAMC recibe la información, debe ingresarla al portal del BPS, originándose de esta forma la solicitud de subsidio por enfermedad del trabajador.

Este sistema fue fuertemente cuestionado por el Sindicato Médico del Uruguay, por entender que obligaba a los médicos a violar el secreto profesional. Cómo lo señala el Prof. Carlos Delpiazzo en informe al respecto "al anotarse en el formulario la patología del paciente, no se está haciendo otra cosa más que dando a conocer por parte del médico el diagnóstico realizado al paciente"[18]. Citando doctrina argentina, agrega, que en el caso del médico que va a certificar a un empleado, éste "debe consignar que por razones médicas se haya impedido de cumplir funciones en un área específica o en el ámbito laboral en su totalidad no estando autorizado a divulgar el motivo[19]".

Concluye el referido Profesor que "El diagnóstico es un elemento comprendido en el secreto médico y por tanto el médico está obligado a no divulgarlo a nadie so pena de cometer delito, salvo en los casos excepcionales previstos por la ley. En función de ello, el médico está impedido de consignar públicamente el diagnóstico y no puede ser obligado a ello por su empleador en tanto este último no puede obligarlo a cometer delito".

A partir de la postura del colectivo médico y sus asesores jurídicos, en los formularios de certificación aludidos se solicita la firma del paciente autorizando que la información contenida sea remitida al BPS, a los efectos requeridos en su certificación laboral, y se consigna al dorso la siguiente leyenda: "La presente certificación de enfermedad se expide a expresa solicitud de la persona identificada como "Solicitante", a los solos efectos que el BPS tramite su solicitud de subsidio por enfermedad que inicia o continúa en este acto y será utilizada sólo para los propósitos del Sistema Nacional de Certificación Laboral, administrado por el BPS para la tramitación y pago del beneficio solicitado por los trabajadores de la actividad privada comprendidos en el Decreto-Ley N° 14.407 de 22 de julio de 1975, pudiendo hacerse extensivo, previa resolución del Directorio, a los propios funcionarios del Organismo.

---

17 Cuyo sustento normativo se encuentra en el artículo 15 de la Ley N° 18.211 de 5 de Diciembre de 2007, que dispuso que la Junta Nacional de Salud suscribiría un Contrato de Gestión con cada uno de los prestadores que integrasen el Sistema Nacional Integrado de Salud, cuyo contenido sería determinado por la reglamentación. Por Decreto del Poder Ejecutivo N° 464/2008 de 2 de Octubre de 2008, se aprobó el proyecto de Contrato de Gestión entre la JUNASA y cada prestador integral. A partir de lo cual, el BPS instauró el Sistema Nacional de Certificación Laboral.

18 Disponible en www.smu.org.uy, visita realizada el 2 de Mayo de 2013.

19 Disponible en www.smu.org.uy, visita realizada el 2 de Mayo de 2013. Referencia a Roberto Foyo. El secreto profesional como elemento del acto médico. Revista SIDEME, n° 3, 2010.

Es deber del solicitante informarle a la empresa que se ha certificado por enfermedad, ya que la misma deberá -a través de los mecanismos que el BPS pone a su disposición- ingresar el resto de los datos necesarios para completar el trámite del otorgamiento de la prestación y consecuentemente con ello su habilitación al cobro. No obstante NO DEBERA ENTREGAR ESTE CERTIFICADO A LA EMPRESA." (se aclara que el resaltado y la mayúscula son del texto original).

De esta forma, se laudó la controversia relativa a los certificados del Sistema Nacional de Certificación Laboral, reconociéndose que el diagnóstico está amparado en el secreto médico y su revelación procede solo a instancia del paciente.

6. Forma de comunicación. Corresponde distinguir dos hipótesis, relativas a la forma en que los trabajadores con certificación médica deben comunicar tal extremo a sus empleadores:

6.1 Los trabajadores amparados en el régimen del BPS, deberán informarle a la empresa que han sido certificados por enfermedad y no deberán entregar el certificado en el cual consta el diagnóstico, a la empresa.

6.2 Los trabajadores no amparados en el régimen del BPS, deberán presentar el certificado médico sin el diagnóstico, siendo suficiente la indicación de reposo del profesional actuante.

III. Conclusiones

1. Desde el punto de vista médico, el diagnóstico está amparado en el secreto profesional, regulado en el artículo 302 del Código Penal. Su relevamiento, procede únicamente por justa causa, obligación legal o autorización expresa y escrita del paciente.

2. Desde el punto de vista del paciente, el diagnóstico es información sensible, especialmente protegida por la Ley de Protección de Datos Personales, y su comunicación procede únicamente, mediante su autorización expresa y por escrito.

3. En consecuencia, no resulta ajustado a derecho, que el empleador exija la inclusión del diagnóstico en el certificado médico laboral.

Es todo cuanto tengo que informar.

Firmado:

Dra. Bárbara Muracciole
Derechos Ciudadanos

Informe N° 94, de 8 de mayo de 2013.

Se informa consulta realizada acerca de la pertinencia de incluir datos personales de profesionales en un catálogo que llevará el Ministerio de Salud Pública.

INFORME No.		EXPEDIENTE No.
94	2013	2013-2-10-0000177

Montevideo, 8 de mayo de 2013

I. Antecedentes

En el marco del Programa Salud.uy, se trata de disponibilizar en línea los catálogos del Ministerio de Salud Pública (MSP), a los efectos de estandarizar los diferentes códigos utilizados en el área y que los prestadores de salud puedan construir historias clínicas electrónicas interoperables. Entre dichos catálogos se encuentra el de los profesionales de la salud habilitados por el MSP. Se consulta a la URCDP, acerca de la posibilidad de comunicar estos datos personales. El público objetivo o destinatario de esta información serían los Efectores del Sistema Nacional Integrado de Salud – SNIS (se entiende que efectores refiere a los prestadores de servicios públicos y privados que integran el sistema).

La información que reside en el catálogo es la siguiente:

- Cédula de Identidad
- Nombres y Apellidos
- Fecha de nacimiento
- Sexo
- Si es profesional médico o no
- Si está habilitado a ejercer o no
- Número de caja profesional si posee.

Las consultas se realizarían:

. Por número de cédula de identidad
. Por datos patronímicos
. Por número de caja profesional.

II. Análisis de la comunicación de datos y sus excepciones

La consulta refiere a la comunicación de datos personales que según define la Ley N° 18.331 es toda revelación de datos realizada a una persona distinta del titular.

En el caso que se consulta, esta comunicación sería realizada por el MSP a los prestadores de servicios que integran el SNIS. La Ley N° 18.211 sobre el Sistema Nacional Integrado de

Salud, establece en el art. 2° que compete al Ministerio de Salud Pública la implementación de este sistema que articulará a los prestadores públicos y privados de atención integral a la salud, determinados en el art. 265 de la Ley Nº 17.930, de 19 de diciembre de 2005. En este artículo se establece que éstos serían las instituciones de asistencia médica colectiva previstas en el art. 6º de la Ley Nº 15.181, así como las instituciones de asistencia médica privada particular sin fines de lucro, así como los seguros integrales autorizados y habilitados por el Ministerio de Salud Pública.

Por otra parte, el art. 17 establece al respecto que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo.

Creemos que en el caso es perfectamente aplicable lo antes expresado, pues en definitiva los datos serán comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario. En el caso del MSP, es de su interés cumplir con los cometidos legales asignados por la Ley a efectos de garantizar el funcionamiento del Sistema, así como en cuanto a los profesionales, es de su interés que sus servicios sean contratados, para lo cual es necesario que cierta información, tanto la relativa a la identidad como a la referida a sus acreditaciones profesionales, sean conocidas por quienes operan en el sistema.

Hay que tener presente, que al respecto la Ley N° 18.335 de Derechos y Obligaciones de Pacientes y Usuarios de los Servicios de Salud establece además que todo paciente tiene derecho a una atención en salud de calidad, con trabajadores de salud debidamente capacitados y habilitados por las autoridades competentes para el ejercicio de sus tareas o funciones (art. 7°), así como que también tiene derecho a conocer todo lo relativo a su enfermedad, comprendiendo entre otras cosas, el derecho a conocer quién o quiénes intervienen en el proceso de asistencia de su enfermedad, con especificación de nombre, cargo y función (art. 18).

A su vez, el art. 17 de la Ley N° 18.331, además de requerir el interés legítimo del emisor y del destinatario, establece una serie de excepciones a la exigencia del previo consentimiento informado del titular del dato. Analizaremos a continuación aquellas que aplican a este caso:

a) Que así lo disponga una ley de interés general. En la consulta de referencia existen normas habilitantes como la Ley N° 18.211 y la Ley N° 18.335, entre otras. Esta excepción se relaciona también con la establecida en el art. 9º B), que establece que no se requiere solicitar el consentimiento cuando los datos se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. En este caso, tanto el MSP como los prestadores de servicios públicos deben tratar estos datos para cumplir con sus funciones, así como los privados deben atender a ciertas obligaciones legales.

b) En los supuestos del art. 9° corresponde entonces considerar que éste en su lit. C)

establece que “No será necesario el previo consentimiento cuando se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento”.
Para el resto de los datos que se comunicarán (si es profesional médico o no, si está habilitado a ejercer o no, y el N° de Caja Profesional), rigen las demás excepciones previstas en el art. 17 y antes analizadas, pero además aplica otros de los supuestos del art. 9°. Efectivamente, en el lit. D) de éste se establece que no se requiere recabar el previo consentimiento para tratar los datos, cuando éstos deriven de una relación contractual, científico o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.
En este sentido, como ya se había indicado antes, en definitiva los profesionales de la salud han celebrado un contrato laboral o científico, que requiere que algunos de sus datos personales sean comunicados para que éste pueda ser desarrollado en interés de ambas partes.

III. En conclusión

El MSP no requiere recabar el previo consentimiento informado de los profesionales de la salud, para comunicar los datos indicados en la consulta que se formula, en el marco de las obligaciones establecidas en la Leyes N° 18.211 y Nº 18.335, pues aplican al caso las excepciones previstas en los arts. 9° lits. B), C) y D), y 17 lits. A) y B) de la Ley N° 18.331.
La comunicación de los datos se debe realizar en el marco del SNID y a los efectores debidamente autorizados por el MSP.
Es importante considerar que el destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y responderá solidaria y conjuntamente por la observancia de la Ley ante la URCDP.

Firmado:
Dra. Graciela Romero
Derechos Ciudadanos

Informe N° 116, de 24 de mayo de 2013.

Se informa consulta respecto a la adecuación de una base de datos de recomendaciones empresariales al marco legal dado por la Ley Nº 18.331.

INFORME No.		EXPEDIENTE No.
116	2013	2013-2-10-0000219

Montevideo, 24 de mayo de 2013

I. Antecedentes

El Sr. Guillermo Winkler consulta acerca de si su proyecto se adecua o no, al marco legal establecido por la Ley N° 18.831.

Dicho proyecto se trata de un sistema de referencias empresariales, donde cada empresa afiliada al mismo, podrá ingresar cédula y nombre del empleado y una evaluación numérica que indique si lo recomienda o no lo recomienda. La empresa podrá reservarse el derecho de no establecer ninguna opinión sobre la persona evaluada, e ingresar un número de teléfono para que la referencia (o sea la empresa) sea consultada por vía telefónica.

Para poder consultar las referencias incluidas en el sistema, las empresas deberán estar afiliadas al mismo y obtener el consentimiento previo de las personas, que les proveerán con cédula de identidad para que se pueda realizar la búsqueda.

El sistema no permite emitir listados ni navegar la información de personas que no hayan brindado el consentimiento para la consulta.

También se proveerá de un mecanismo para que las personas soliciten que su información sea rectificada, actualizada o suprimida, cumpliendo así con el art. 15 de la Ley.

II. Análisis y marco jurídico de aplicación

El art. 17 de la Ley establece que los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario, y con el previo consentimiento del titular de los datos.

En el caso que se consulta, evidentemente existe interés legítimo, tanto del emisor como del destinatario, pero no se puede inferir el consentimiento del contexto de la relación laboral o contractual, ni de la entrega de la C.I. por parte del trabajador, pues el sistema que instituye la Ley no se basa en el consentimiento tácito sino en el consentimiento expreso (art. 9° primera parte).

En este sentido, si bien en el art. 9° D) de la Ley se establece una excepción al consentimiento cuando los datos “deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento”, en el caso hay que diferenciar entre la relación laboral o contractual en sí, y la posibilidad de ser incluido en esta base de datos de referencias empresariales.

Esta distinción es relevante, pues permite concluir que la inclusión en este sistema en definitiva no es necesaria para el desarrollo o cumplimiento de la relación laboral o contractual de que se trate, -exigencia prevista en el art. 9° D)-, por ende, debe solicitarse el consentimiento en

forma expresa, ya sea mediante un formulario o una cláusula específica.
Por otra parte, los trabajadores cuyos datos van a estar ingresados en el sistema y eventualmente serán comunicados, deben ser informados de la finalidad de la base y de esa eventual comunicación, en los términos establecidos en el art. 13 de la Ley.
En cuanto a la calificación emitida por la empresa, acerca de si lo recomienda o no, la misma deberá ser lo más objetiva posible, sin incluir juicios de valor que puedan vulnerar la integridad de las personas, y sin incluir datos sensibles que puedan llegar a constituirse en una forma de discriminación.
En este sentido, es fundamental considerar lo establecido en el art. 7° de la Ley: "Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación a la finalidad para la cual se hubiesen obtenido". Además, "la recolección (...) no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones" de la Ley.
En definitiva, si la recomendación de la empresa, se realiza en forma numérica, siendo adecuada y proporcionada, y además se cuenta con el consentimiento de los interesados, cabe concluir que en principio, no se estaría vulnerando la norma.

III. Sobre la observancia de los demás principios de la Ley

Corresponde tener presente también, que aplican al tratamiento de los datos los demás principios que inspiran la Ley, sobre todo y especialmente, los de finalidad, confidencialidad y seguridad, los cuales a su vez, servirán de criterio interpretativo para resolver las cuestiones que puedan suscitarse.
Además, la base de datos que se forme deberá ser inscripta en el registro de la URCDP, tal como se establece en el art. 6° de la Ley (Principio de Legalidad).

IV. Conclusiones

A la luz de los antes analizado, según lo planteado en la consulta, cabe concluir que:

a) Para que los datos de los trabajadores puedan ser incluidos en el sistema debe recabarse el consentimiento en forma expresa mediante un formulario o cláusula específica que debe ser firmada por los mismos, conforme lo establecido en el art. 9° de la Ley.

b) Además, los interesados (trabajadores o empleados) deberán ser informados en los términos previstos en el art. 13 de la Ley, así como el responsable de la base deberá adoptar las medidas de seguridad adecuadas a efectos de garantizar la confidencialidad y la reserva de los datos proporcionados.

c) A su vez, deberán observarse en el tratamiento y la recolección de los datos los demás principios que estructuran la Ley, especialmente los de Finalidad y Proporcionalidad, así como se deberá inscribir la base de datos en el registro de la URCDP, dentro de los 90 días siguientes a su creación.

Firmado:

Dra. Graciela Romero

Derechos Ciudadanos

Informe Nº 123, de 5 de junio de 2013.

Se informa consulta sobre el alcance de las palabras “listados” y “medios” utilizadas en el artículo 9º C) de la Ley Nº 18.331 y en los artículos 3º B) y 9º D) del decreto Nº 414/009.

INFORME No.		EXPEDIENTE No.
123	2013	2013-2-10-0000230

Montevideo, 5 de junio de 2013

I. Antecedentes

1. La Comisión de Protección de Datos Personales de la Contaduría General de la Nación, formula consulta sobre el alcance de las palabras “listados” y “medios”, utilizadas en el lit. C) del art. 9º de la Ley N° 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data, y el lit. B) del art. 3º del decreto N° 414/009 de 31 de Agosto de 2009 respectivamente, así como sobre la exigencia de motivación para el ejercicio de los derechos, solicitada en el lit. D) del art. 9º del mismo decreto.

2. Corresponde a la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) evacuar la consulta, en mérito al cometido de asistencia y asesoramiento, que le fuera atribuido por el art. 34 lit. A) de la Ley N° 18.331.

II. Análisis

3. Interpretación.- A los efectos de dar respuesta a la consulta planteada, corresponde acudir a las reglas de interpretación de la Leyes, establecidas en el Título Preliminar del Código Civil. Particularmente, a los arts. 17 inc. 1 y 18 que señalan que “Cuando el sentido de la ley es claro, no se desatenderá su tenor literal, a pretexto de consultar su espíritu”, y que “Las palabras de la ley se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras; pero cuando el legislador las haya definido expresamente para ciertas materias, se les dará en éstas su significado legal”.

4. Listados.- Siguiendo las premisas antes citadas, encontramos que la palabra “listados” no ha sido definida expresamente por el legislador en materia de protección de datos personales, por lo que debe ser entendida en su sentido natural y obvio, según el uso general. De acuerdo con La Real Academia Española, listado viene del participio listar, que significa formar o tener listas. Lista, se define como “la enumeración, generalmente en forma de columna, de personas, cosas, cantidades etc., que se hace con determinado propósito”[20].
En este sentido, debe entenderse por listados al tenor del lit. C) del art. 9º de la Ley de Protección de Datos, toda expresión sucesiva, cómputo o cuenta numeral, de los datos enunciados en

20 Información disponible en http://lema.rae.es/drae/?val=listados. Consulta realizada el 4 de Junio de 2013.

dicha norma, independientemente de la forma adoptada (desde que el adverbio de modo, generalmente, es enunciativo de la mayoría de los casos, pero no excluyente de otras formas).

5. Medios.- Siguiendo igual razonamiento, encontramos que la palabra “medios” no ha sido definida expresamente por el legislador en materia de protección de datos personales, por lo que debe ser entendida en su sentido natural y obvio, según el uso general.

De acuerdo a la Real Academia Española, medio es la “cosa que puede servir para un determinado fin” o “diligencia o acción conveniente para conseguir algo”[21]. Esta definición debe ser entendida en sentido amplio, continente de todos los medios existentes al momento de realizarse la interpretación, sean éstos técnicos, humanos, físicos, lógicos, u otros, siempre que permitan establecer un punto de conexión con el territorio nacional y consiguiente aplicación de la ley uruguaya.

6. Motivo de la solicitud.- Al analizar la solicitud de motivación, requerida por el lit. B) del art. 9º del Decreto N° 414/009, a la luz de las disposiciones de la Ley de Protección de Datos Personales, encontramos que se trata de un requisito que excede la norma reglamentada, razón por la cual no puede exigirse como condición para el ejercicio de los derechos de los titulares de datos.

III. Conclusiones

1. A los efectos de dar respuesta a la consulta planteada, corresponde acudir a las reglas de interpretación de la Leyes, establecidas en el Título Preliminar del Código Civil.

2. Las palabras “listados” y “medios”, enunciadas en el lit. C) del art. 9º de la Ley N° 18.331 y en el lit. B) del art. 3º del decreto N° 414/009 respectivamente, no han sido definidas expresamente por el legislador en materia de protección de datos personales, por lo que deben ser entendidas en sus sentidos naturales y obvios, según el uso general.

3. La solicitud de motivación requerida por el lit. B) del decreto N° 414/009, resulta excesiva a la luz de las disposiciones de la Ley de Protección de Datos reglamentada, razón por la cual no puede exigirse como condición para el ejercicio de los derechos de los titulares de datos.

Es todo cuanto tengo que informar.

Firmado:

Dra. Bárbara Muracciole
Derechos Ciudadanos

21 Información disponible en http://lema.rae.es/drae/?val=listados. Consulta realizada el 4 de Junio de 2013.

Informe N° 124, de 7 de junio de 2013.

Se informa consulta realizada de oficio por el Consejo Ejecutivo de la URCDP sobre la publicación de datos personales en el sitio web.

INFORME No.		EXPEDIENTE No.
124	2013	2013-2-10-0000232

Montevideo, 7 de junio de 2013

I. Antecedentes

El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, consulta sobre cierta publicación de información de los estudiantes, en la web de la Facultad de Ingeniería de la Universidad de la República.

II. Análisis

A. Generalidades

1. Herramienta Diagnóstica al Ingreso (HDI).- Desde el año 2005, la Facultad de Ingeniería aplica una Herramienta Diagnóstica al Ingreso (HDI) con carácter obligatorio para la totalidad de los estudiantes. Esta herramienta tiene como objetivo principal, realizar un análisis global de cada generación, permitiendo a su vez a cada estudiante una autoevaluación y a los docentes de los primeros cursos, un acercamiento inicial a las competencias que traen sus estudiantes cada año.

Se evalúan competencias y desempeños en áreas cuyo dominio se considera esencial para comenzar la carrera, como Física, Matemática, Química, Comprensión Lectora y Expresión escrita.

En base a los resultados obtenidos, se elaboran informes estadísticos sobre las condiciones académicas de los estudiantes, al Ingreso de la Facultad de Ingeniería. Además, se otorgaran 5 puntos máximos, graduados en forma proporcional a los resultados globales obtenidos por el estudiante en las Actividades 1 y 2 de la Prueba Diagnóstica. Es decir, que de acuerdo al resultado obtenido, a cada estudiante se le podrá otorgar hasta un máximo de 5 puntos en cada una de las asignaturas a las que se inscriba en el primer semestre de la carrera, que se sumarán al puntaje obtenido por el estudiante, tanto para la aprobación como para la exoneración del curso en cuestión.

Los resultados se publican el sitio web de la Facultad de Ingeniería, discriminando el nombre del estudiante, su cédula de identidad, el resultado y los puntos obtenidos.

B. Publicación de resultados

2. Comunicación de datos.- Esta publicación, se enmarca en la definición legal de comunicación de datos personales dada por la Ley N° 18.331, de 11 de Agosto de 2008,

de Protección de Datos Personales y Acción de Habeas Data, desde que se trata de una "revelación de datos realizada a una persona distinta del titular de datos". La cual, en principio, deberá contar con el previo consentimiento informado de sus titulares.

Corresponde por tanto revisar, si ha sido consentida o se enmarca dentro de alguna de las excepciones previstas para poder comunicar datos personales sin consentimiento de sus titulares, en el entendido que aún así, subsistirá el requisito del interés legítimo.

2.1 Publicación de resultados.- Según se desprende del Reglamento General de Estudios, de la Facultad de Ingeniería, en su art. 40, los resultados de las pruebas serán publicados. Si bien esta norma fue dictada para pruebas de conocimiento relacionadas a la currícula de grado y postgrado, es absolutamente aplicable y extensible a la examinación que nos ocupa, desde que la misma culmina con atribución de puntaje que repercute directamente en las materias curriculares.

Ingresar a una casa de estudios, implica una conducta positiva de aceptación de su reglamento de funcionamiento, y equivale al consentimiento expreso, en la especie, a la publicación de resultados.

2.2 Excepciones.- Sin perjuicio de lo expuesto en el numeral anterior, entiendo que estamos ante un caso de excepción al consentimiento informado, en aplicación de los lits. C) y B) del art. 9º, y D) del art. 9º bis de la Ley N° 18.331.

En efecto. La Facultad de Derecho de la Universidad de la República, obtiene los datos en ejercicio de la función administrativa para el cumplimiento de su cometido social de impulsar la enseñanza y en virtud de lo dispuesto en la Ley Orgánica de la Universidad de la República y su Reglamento Interno.

Por otra parte, conocer los resultados y puntajes asignados, resulta de interés de los examinados, como forma de contralor hacia el actuar de la Facultad. Lo que nos introduce en la necesaria transparencia que debe signar los actos de la Universidad de la República.

2.3 Transparencia.- La Facultad de Ingeniería de la Universidad de la República, en cuanto persona pública estatal, es responsable de promover la transparencia en la función administrativa, conforme lo preceptuado en el art.1º y demás disposiciones de la Ley N° 18.381, de 17 de Octubre de 2008, de Acceso a la Información Pública.

En este sentido, la publicación de los resultados que nos ocupan y asignación de puntaje correspondiente, resulta determinante a fin de mantener la transparencia y consecuente control legalmente requeridos, fundamento estos últimos, de la finalidad y del interés legítimo exigidos por la Ley de Protección de Datos Personales en sede de comunicación.

2.4 Finalidad y veracidad.- Todo lo antedicho respecto de la publicidad de los datos bajo análisis, debe enmarcarse en función de los principios de finalidad y proporcionalidad. En este sentido, se aprecia que la publicación en la web de la Facultad de Ingeniería, accesible a cualquier persona, resulta excesiva en relación a la finalidad de transparencia, pudiendo perjudicar a los alumnos involucrados. Máxime cuando existen informes estadísticos (disociados), que son el producto verdaderamente útil de este proceso,

tanto para la Universidad de la República como para la sociedad en general.
Las personas interesadas en conocer los resultados nominados, son los examinados mediante la herramienta de HDI, y no el público en general, el cual puede mal interpretar los datos por desconocimiento, y formar opinión equivocada sobre las aptitudes de algún estudiante. Pensemos por un instante en las consultas web que realizan los potenciales empleadores y las empresas intermediarias de recursos humanos.
Esta desproporción puede salvarse, por ejemplo, manteniendo la información accesible solo a los interesados, mediante usuario y contraseña.

III. Conclusiones

1. El presente informe refiere a la publicación en el sitio web de la Facultad de Ingeniería de la Universidad de la República, de la lista de estudiantes, cédula de identidad, resultados y puntos asignados, en función de la utilización de la Herramienta Diagnóstica al Ingreso (HDI). No aborda ni se pronuncia, sobre la pertinencia, uso y obligatoriedad de la misma.

2. Se trata de una comunicación de datos excepcionada del requisito del previo consentimiento informado de su titular, conforme lo dispuesto en los lits. C) y B) del art. 9º y D) del art. 9º bis de la Ley N° 18.331.

3. Responde a la responsabilidad legal de la Facultad de Ingeniería de la Universidad de la República, de promover la transparencia en la función administrativa, conforme lo dispuesto en el art. 1º y demás disposiciones de la Ley N° 18.381.

4. No obstante, la publicación en la web accesible por el público en general, resulta excesiva en relación a la finalidad de transparencia, por lo que se sugiere recomendar a la Facultad de Ingeniería mantener la información bajo usuario y contraseña.

Es todo cuanto tengo que informar.

Firmado:
Dra. Bárbara Muracciole
Derechos Ciudadanos

Informe N° 126, de 20 de junio de 2013.

Se informa consulta acerca del carácter de confidencialidad que poseen los datos personales de firmas pertenecientes a empresas de despachantes de aduana.

INFORME No.		EXPEDIENTE No.
126	2013	2012-2-10-0000768

Montevideo, 20 de junio de 2013

I. Antecedentes

1. La Asociación de Despachantes de Aduana del Uruguay (ADAU), consulta sobre la aplicación del art. 10 de la Ley N° 18.331, de 11 de Agosto de 2008, de Protección de Datos Personales y Acción de Habeas Data, en el marco de la Ley N° 18.694 de 21 de Octubre de 2010, su decreto reglamentario N° 43/2011 de 01 de Febrero de 2011 y Orden del Día de la Dirección Nacional de Aduana N° 32/2011 de 14 de Abril de 2011.

2. Previo ingreso al análisis, se deja constancia que si bien la consulta fue presentada ante la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP), en su primer párrafo se dirige a la UCE (Unidad de Certificación Electrónica). Del cuerpo del escrito se desprenden dos temas centrales que son: la aplicabilidad del art. 10 de la Ley de Protección de Datos y la necesidad de encriptación de la información transmitida.

3. Corresponde a la URCDP evacuar la consulta en materia de protección de datos, en mérito al cometido de asistencia y asesoramiento que le fuera atribuido por el art. 34 lit. A) de la LPDP. No así, sobre la necesidad de encriptación, materia que se encuentra fuera de su competencia.

II. Análisis

4. Consideraciones Generales.- A partir de la Ley N° 18.694 y su Decreto reglamentario N° 43/2011, los despachantes de aduana, en su calidad de agentes privados de interés público, deberán guardar, conservar y archivar todos los documentos, cualquiera sea su soporte, relativos a las operaciones aduaneras, en las que hayan intervenido como tales. A tales efectos y bajo su estricta responsabilidad, podrán contratar los servicios de terceros, previa autorización de la Dirección Nacional de Aduanas (DNA).

La guarda conservación y archivo será exigible por un plazo de diez años, contados a partir de la fecha de numeración de la declaración, debiendo hacerlo dentro de los primeros cinco años en soporte original en papel y como documento electrónico, pudiendo luego de ese período archivarlos solo electrónicamente.

A tales efectos, los despachantes podrán contratar, bajo su estricta responsabilidad, los servicios de terceros para guardar, conservar y archivar los documentos relativos a las operaciones aduaneras. Los terceros interesados así como los despachantes, deberán contar

con la autorización previa de la DNA.
Mediante estas normas, se crea y se regula específicamente un sistema de guarda, conservación y archivo de la documentación aduanera constitutivo de bases de datos.

5. Aplicación de la Ley N° 18.331.- El art. 3º lit. C) de la Ley N° 18.331, dispone que la norma no será de aplicación a las bases de datos "creadas y reguladas por leyes especiales". En este sentido, las bases de datos creadas y reguladas por la Ley y el Decreto que nos ocupan, se encuentran excluidas del ámbito de aplicación de la Ley de Protección de Datos Personales. Por lo que la respuesta a la consulta planteada debe ser negativa.

6. Principios.- El art. 10 de la Ley de Protección de Datos Personales, recoge el principio de seguridad de los datos, que implica la adopción de las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales, con el fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y detectar desviaciones de información.
Si bien no resulta aplicable al caso que nos ocupa, en cuanto conjunto de ideas rectoras, los principios deberán estar presentes siempre que estemos ante tratamiento de datos personales, como garantes de posibles excesos contra sus titulares.

7. Seguridad.- En este sentido, de la normativa aduanera analizada, se desprende la contemplación del principio de seguridad aludido, desde que el Art. 5 del decreto reglamentario relativo a la "Conservación de la Documentación", específicamente regula el deber de conservación e integridad, mandatando evitar su sustracción, destrucción o deterioro.

III. Conclusiones

1. La ADAU consulta sobre la aplicabilidad del art. 10 de la Ley N° 18.331, en el marco de las normas específicas que regulan la guarda, conservación y archivo de los documentos aduaneros.

2. El mencionado artículo no se aplica a las bases de datos creadas y reguladas por la Ley N° 18.694 y Decreto N° 43/201, las que se encuentran excluidas del ámbito de aplicación de la Ley de Protección de Datos Personales.

3. Sin perjuicio, las normas relacionadas contemplan el principio de seguridad, desde que el art. 5º del Decreto reglamentario específicamente regula el deber de conservación e integridad de la documentación aduanera, mandatando evitar su sustracción, destrucción o deterioro.

4. No corresponde a la URCDP pronunciarse sobre la necesidad de encriptación, por tratarse de materia fuera de su competencia.

Es todo cuanto tengo que informar.

Firmado:
Dra. Bárbara Muracciole
Derechos Ciudadanos

Informe Nº 184 de 13 de setiembre de 2013.

Se informa consulta acerca de la elaboración del contenido de un pliego sobre un proyecto que comprende la inclusión de una cédula electrónica.

INFORME No.		EXPEDIENTE No.
184	2013	2013-2-10-0000391

Montevideo, 13 de setiembre de 2013

I. Antecedentes

La Ing. Sabrina Trotta Mouriño de la Secretaría - Departamento de Informática del Ministerio del Interior presenta la siguiente consulta:

"El Ministerio del Interior está trabajando en la elaboración del pliego de un proyecto que comprende la inclusión de una cédula de identidad electrónica. Con respecto a la CI, el objetivo es que la misma sea un documento de viaje conforme con ICAO 9303.

La misma presentará información visible (como hasta ahora) e información digital almacenada en chips de dos tipos: uno con contacto y otro sin contacto. El chip con contacto para ser leído requiere entrar en contacto con un dispositivo de lectura, mientras que el chip sin contacto puede ser leído con un dispositivo de lectura autorizado a una distancia máxima de 10 cm entre lector y CI.

La consulta que queremos realizarles se refiere a los datos personales que se pueden (o no se pueden) almacenar en el chip sin contacto. Los datos que ICAO 9303 ha determinado como obligatorios son los siguientes:

- Tipo de documento
- Estado u organismo expedidor
- Nombre (del titular)
- Número de documento
- Dígito de control - número de documento
- Nacionalidad
- Fecha de nacimiento
-Dígito de control - fecha de nacimiento
-Sexo (de nacimiento (N) y sexo actual (A), en formato N/A)
-Fecha de expiración o válido hasta
-Dígito de control - Fecha de expiración o válido hasta
-Rostro

Las principales dudas nos surgen con los datos marcados en color naranja".

II) Análisis y marco jurídico de aplicación

1. Sexo (de nacimiento (N) y sexo actual (A), en formato N/A)

Efectivamente uno de los datos referidos en la consulta, señalado en color naranja, refiere al sexo actual y sexo anterior de la persona, lo cual constituye un dato sensible.

Como regla, los datos de origen racial o étnico, -por ser datos sensibles-, sólo pueden ser objeto de recolección y tratamiento con consentimiento expreso y escrito del titular o cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo.

No obstante hay que tener presente que existe la obligación a cargo de los Estados de actuar instrumentando las medidas y políticas necesarias y adecuadas, para garantizar y proteger los derechos humanos de todas las personas, (incluyendo ello su seguridad)y precisamente, la Ley Nº 18.331 en su artículo 18 establece que, los "datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo."

Según se infiere de la consulta, se trata de cumplir con las funciones que posee el Ministerio del Interior en materia de seguridad pública, para lo cual necesita identificar en forma lo más certera posible a todas las personas, especialmente en lugares de entrada y salida del país como son los aeropuertos.

Se indica además en la consulta, que los datos solicitados se enmarcan en el Documento ICAO 9303 que se trata de un documento elaborado por la Organización de Aviación Civil Internacional, que habla sobre las características que deben tener los documentos de viaje de lecturas mecánicas.

Es importante considerar que parte de este documento (en especial sus especificaciones técnicas), ha recibido la aprobación de la Organización Internacional de Normalización con carácter de normas ISO 7501-1, 7501-2 y 7501-3 (http://www.icao.int/publications/Documents/9303_p3_v1_cons_es.pdf).

2. Rostro

En cuanto al rostro, -otro dato señalado con color naranja-, cabe destacar que se trata de un dato biométrico. La biometría tiene dos funciones claramente delimitadas: la verificación y la identificación. Precisamente el reconocimiento facial es una aplicación dirigida por un programa informático destinado a identificar automáticamente a una persona en una imagen digital, mediante la comparación de determinadas características faciales existentes en una base de datos. Se recomienda el uso de la biometría al sólo efecto de verificación.

En razón de ello, como muy bien lo expresa el G29 "los elementos biométricos en los pasaportes, en otros documentos de viaje o en los carnés de identidad son muy sensibles. Por tanto hay que garantizar que sólo las autoridades competentes pueden acceder a los datos

almacenados en el chip".
Es por ello que a este fin, el Grupo de trabajo ha apoyado la petición del Parlamento Europeo de que cada Estado miembro de la UE, mantenga un registro de las autoridades competentes y de órganos autorizados. Los Estados comunicarán este registro y, en caso necesario, las actualizaciones regulares, a la Comisión Europea, que mantendrá un registro en línea actualizado, publicando cada año una compilación de los registros nacionales (Grupo de Trabajo Art. 29. Informe 3/2009 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_es.pdf)
El tema es tan delicado desde el punto de vista de la protección de datos, que el Grupo de Trabajo expresa en su informe también, que el Parlamento Europeo solicitó que el pasaporte incluyera un soporte de almacenamiento muy seguro, con la suficiente capacidad y apto para salvaguardar la integridad, autenticidad y confidencialidad de los datos almacenados.
Agregan que estos riesgos "necesitan una arquitectura de seguridad que aspire a proporcionar un nivel cada vez mayor de confianza para el intercambio de información", es por ello que consideran necesario el establecimiento de una Infraestructura de Clave Pública Global (PKI), para habilitar el intercambio de esta información, que afortunadamente Uruguay ya tiene (Ley N° 18.600 de Documento y Firma Electrónica y su Decreto 436 de 8 de diciembre de 2011.
En resumen, la inclusión de datos biométricos implica la obligación de garantizar los derechos ante los riesgos que se derivan del uso de la tecnología. Ello refiere a la necesidad de utilizar sistemas seguros, que impidan que se no memoricen rostros por parte de terceros no autorizados y que el acceso a las imágenes de reconocimiento facial esté restringido sólo a las autoridades competentes.
En definitiva, es fundamental introducir las garantías necesarias desde el primer momento de la implantación técnica y conforme lo establezcan los expertos (Informe Jurídico N° 80 del Dr. Marcelo Bauzá publicado en Libro de Resoluciones y Dictámenes de la URCDP año 2009, págs 111 a 125).

La URCDP ya se ha pronunciado respecto a temas similares. Por ejemplo en el Dictamen N° 32, de 27 de diciembre de 2011, en relación con la necesidad que el titular de una cédula de identidad preste su consentimiento para entender que es conforme a derecho la generación del servicio de control de identidad de la Dirección Nacional de Identificación Civil.
En el mismo la URCDP expresa que si bien la visualización en pantalla del referido documento en versión electrónica, no resulta violatoria de la Ley Nº 18.331 y, por el contrario, configura una garantía ciudadana, en cuanto a verificar la fidelidad del documento utilizado y coartar el uso de documentos falsos o cambiados. Lo expresado no equivale a permitir tratamientos diversos al indicado, quedando absolutamente inhibida la creación de nuevas bases de datos a partir de la información consignada, a modo de ejemplo almacenar fotografías, firmas o huellas digitales, todo lo cual requeriría el previo consentimiento informado de los titulares de los datos, para cualquier otro tipo de tratamiento diferente al descripto, incluyendo la

comunicación o cesión de datos.
A su vez, en el Dictamen N° 4/2013, del 16 de mayo de 2013 se emite opinión respecto a una consulta formulada por el Ministerio de Relaciones Exteriores (MRREE) sobre la adecuación de un Proyecto de Convenio interinstitucional que se realizará con la Dirección Nacional de Identificación Civil y que consiste en facilitar una conexión en modalidad “web service” al Servicio SIDECO que proporciona ésta última.
En dicho dictamen se reitera que si bien la simple visualización electrónica de la información contenida en una cédula de identidad, constituye un proceso necesario para validar un acto de identificación, y es conforme al marco regulatorio de la protección de datos personales, es necesario e imprescindible que los organismos responsables tomen “las previsiones del caso (principio de seguridad de los datos, art. 10 de la Ley), respeten la confidencialidad (principio de reserva, art. 11 de Ley), y atiendan el reacomodamiento de eventuales disfunciones que se produzcan (principio de responsabilidad, art. 12 de la Ley)”.

III. Conclusiones y recomendaciones

En definitiva, si bien el art. 3° de la Ley indica que las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado, quedan excluidas del ámbito de aplicación objetivo de la norma, corresponde que desde la perspectiva de un derecho humano que tiene resguardo constitucional y legal como lo es la protección de datos personales, la URCDP realice las siguientes recomendaciones:

a) El desarrollo y la utilización de un mecanismo tecnológico que permita la introducción de garantías tanto desde el punto de vista técnico como jurídico, especialmente en lo referido a:

- que el acceso a los datos del chip esté restringido solamente a las autoridades competentes (que no puedan ser leídos y/o almacenados por terceros ajenos al control de la seguridad pública),

- que los datos sólo puedan ser recogidos y almacenados a los efectos de la seguridad pública y para cumplir con las funciones y cometidos que posee el Ministerio del Interior (Principio de Finalidad y Proporcionalidad)

b) Reserva y Confidencialidad en el tratamiento de este tipo de información y en la operación de todo el sistema, así como se deberán observar los principios de Veracidad, Finalidad, Seguridad de los Datos, y lo establecido respecto a los derechos y obligaciones en general, especialmente lo formulado en el art.18.

Firmado:
Dra. Graciela Romero
Derechos Ciudadanos

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

JOSÉ ARTIGAS
Unión de los Pueblos Libres
BICENTENARIO.UY

agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
REPÚBLICA ORIENTAL DEL URUGUAY