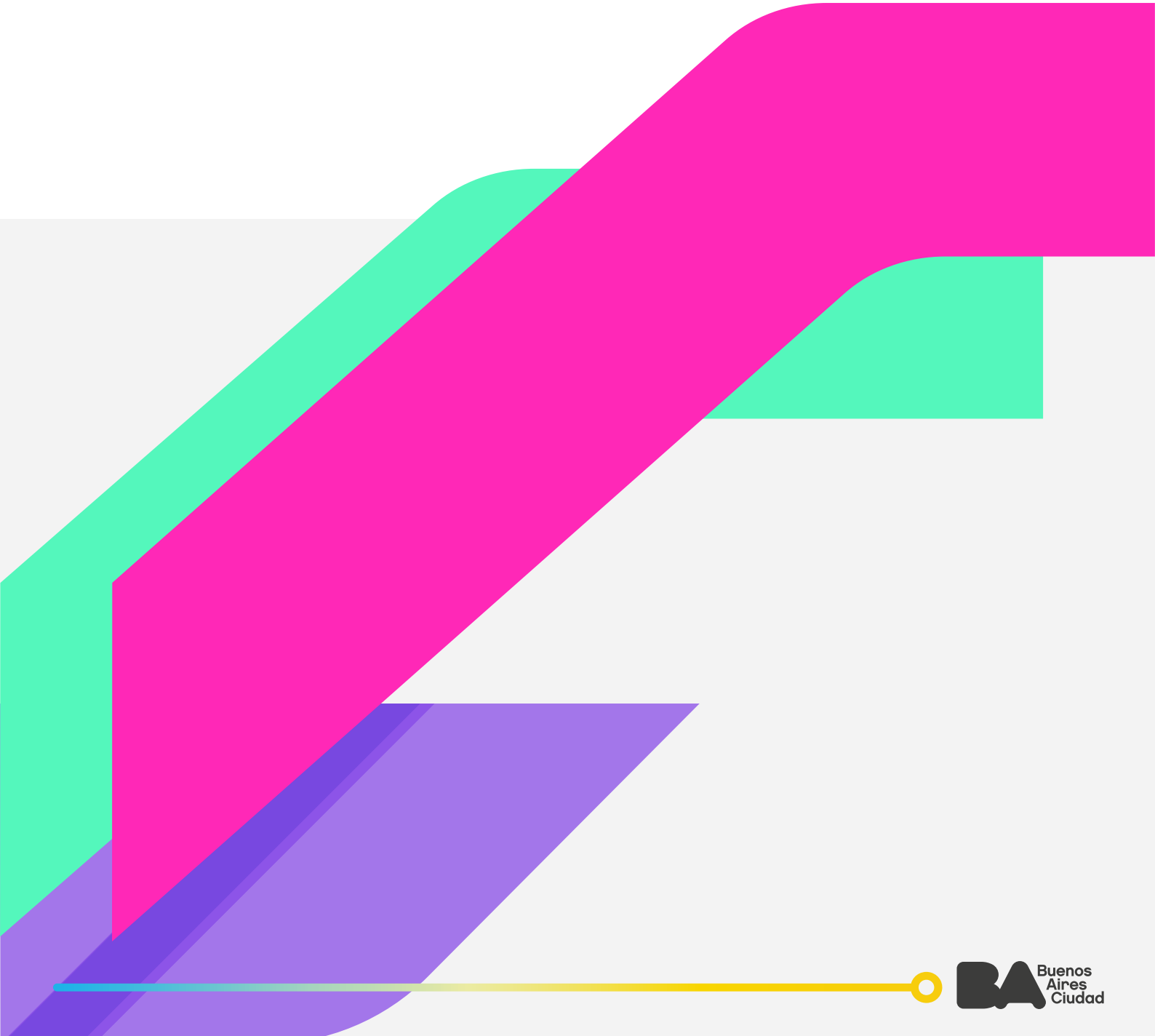
Gobernanza de Datos

Guía de **Clasificación de Datos**

SUBSECRETARÍA DE POLÍTICAS PÚBLICAS BASADAS EN EVIDENCIA
SECRETARÍA DE INNOVACIÓN Y TRANSFORMACIÓN DIGITAL



Buenos Aires Ciudad

Jefe de Gobierno
Horacio Rodríguez Larreta
Jefe de Gabinete
Felipe Miguel
Secretario de Innovación y Transformación Digital
Diego Fernández
Subsecretaria de Políticas Públicas Basadas en Evidencia
Melisa Breda

Índice

1. Introducción

Debido al avance de la tecnología y las herramientas que como Estado tenemos a disposición, se torna cada vez más necesario el tratamiento de datos para alcanzar una administración eficiente, que pueda tomar decisiones basadas en evidencia.

Para ello es esencial una gestión transparente que garantice la confidencialidad, integridad y privacidad de los datos. Ese es el camino que ha comenzado a recorrer la Subsecretaría de Políticas Públicas Basadas en Evidencia con la convicción de que, para generar una transformación real, la misma debe ser acompañada por todas las entidades y jurisdicciones pertenecientes al sector público.

En ese marco, la presente guía busca ofrecer algunos criterios orientadores, en materia de clasificación de datos en el ámbito del sector público del Gobierno de la Ciudad Autónoma de Buenos Aires.

1.1. ¿Qué es y por qué es importante clasificar los datos?

La clasificación de datos es el proceso por el cual se organizan los datos que posee cualquier organización o área en categorías, con el fin de facilitar su tratamiento en función de sus particularidades y normativas específicas.

Es importante destacar que no todos los datos se pueden compartir libremente: algunos tienen requisitos específicos. Identificar estos requerimientos permite realizar una gestión segura y lícita, garantizando la protección de los derechos de todas las personas.

Una clasificación eficiente permite reducir riesgos y responsabilidades en el tratamiento de los datos y garantizar la **seguridad, confidencialidad, integridad, y privacidad de los mismos.**

La presente *guía de clasificación de datos* tiene como objetivo ofrecer **criterios indicadores y orientadores** en el ámbito público del Gobierno de la Ciudad Autónoma de Buenos Aires (en adelante GCABA) sobre **diferentes categorías de datos** en función de su criticidad, contribuyendo a la **adopción de políticas de privacidad y seguridad bajo una perspectiva de riesgo.**

2. Alcance

Sin perjuicio de servir para cualquier persona humana o jurídica, la presente tiene como público objetivo a los organismos que comprenden la **jurisdicción del sector público de la Ciudad Autónoma de Buenos Aires**. Eso es: órganos pertenecientes a la administración central y descentralizada; entes autárquicos; empresas y sociedades del Estado; sociedades anónimas con participación estatal mayoritaria; sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Estado de la Ciudad Autónoma de Buenos Aires tenga participación en el capital o en la formación de las decisiones societarias; Poder Legislativo y Judicial, en cuanto a su actividad administrativa, y en todos los demás órganos establecidos en el Libro II de la Constitución de la Ciudad de Buenos Aires.

2.1.Metadatos, datos e información

En general se definen a los **metadatos** como **datos acerca de los datos**, es decir, **describen el contenido, calidad, condiciones, historia, disponibilidad** y otras características de los mismos. Esto, sin embargo, no alcanza: el tipo de información que se puede clasificar como metadatos es muy amplio. Los metadatos incluyen **información sobre procesos técnicos y de negocio, reglas y restricciones de datos, y estructuras de datos lógicas y físicas.**

En este contexto, podemos decir que **los metadatos** son un caso particular de datos que están asociados a otros, pero que pueden tomarse como **unidad de información, y entran dentro de los mismos criterios de clasificación**.

Es importante destacar que el mismo proceso de clasificación que sufren los datos, comprende a los metadatos.

Se debe aclarar que **utilizar información como sinónimo de dato es incorrecto**, ya que el dato es la representación simbólica de una entidad, como pueden ser números, letras, alfabetos, dibujos, puntos, entre otros; y la información es el conjunto de datos adecuadamente procesados que contribuyen a tomar decisiones basadas en evidencia.

Teniendo en cuenta la importancia que cobran los datos para la política pública y la posibilidad de generar acciones positivas que transformen la vida de las personas, es imprescindible su utilización de manera segura.

3. ¿Cómo se clasifican los datos según su categoría?

Desde los distintos enfoques, niveles y criticidad, podemos destacar las siguientes categorías de datos brindando ejemplos asociados que nos ayudan a comprender cómo se clasifican y en qué contexto:

En este sentido, datos que a simple vista podrían compartirse, en asociación con otros, podrían convertirse en reservados, según el contexto en que se expongan. *Es por ello, que*

más allá de tener en cuenta los lineamientos específicos de esta guía, ***el análisis singular de cada caso es fundamental.***

A continuación se detallarán los tipos de datos existentes, conforme los lineamientos surgientes de la normativa actual:

3.1.Datos públicos:

Se considera dato público a toda aquella información contenida en documentos escritos, fotográficos, grabaciones, soporte magnético, digital o en cualquier otro formato; incluyendo bases de datos, acuerdos, directivas, reportes, estudios, oficios, proyectos de ley, disposiciones, resoluciones, providencias, expedientes, informes, actas, circulares, contratos, convenios, estadísticas, instructivos, dictámenes, boletines o cualquier otra información registrada en cualquier fecha, forma y soporte; que haya sido creada u obtenida por el órgano requerido, y que se encuentre en su posesión y bajo su control.

Ejemplos de datos públicos: Cantidad de expedientes que tramita el GCABA por año, licitaciones, cámaras de seguridad, escuelas públicas, presupuesto asignado a programas; etc.

Dentro de esta categoría se creó una forma de compartir diferentes datos que genera el Estado en formatos abiertos que facilitan su utilización por parte de todas las personas. Los datos que se comparten a través de esos procesos son llamados **datos abiertos.**

3.2.Datos de acceso público irrestricto:

Se entienden por tales a los boletines, medios de comunicación escritos o repertorios oficiales, las guías telefónicas en los términos previstos por su normativa específica; y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección o cualquier otro dato que indique de su pertenencia al grupo.

Las reparticiones que cuenten con datos de fuentes de acceso público irrestricto deberán disponibilizarlos sin ningún requisito previo.

3.3.Datos personales:

A continuación se detallarán los distintos tipos:

3.3.1.Datos personales en general

Son todas aquellas entidades simbólicas que refieren a una persona humana o jurídica determinada o determinable. Se incluyen aquellos relativos a la vida privada y familiar, como así también a las relaciones laborales, actividades económicas o sociales, entre otras.

Ejemplo de datos personales en general: **nombre, DNI, domicilio, edad, fecha de nacimiento, número telefónico, correo electrónico personal, CUIT, características físicas, genéticas o biométricas, patrimonio, trayectoria académica, laboral o profesional.** La característica de que puede ser "determinable" hace referencia a que si bien no se identifica a la persona inequívocamente, por medio de un procedimiento o uniendo diferentes fuentes de datos podría identificarse.

Por ejemplo, una persona puede ser determinada de manera indirecta por:

- La **patente de un vehículo.**
- Un número de teléfono.
- **Consanguinidad** familiar.
- Una combinación de varios criterios significativos **(edad, empleo, domicilio, etc.)**, **que hagan posible su determinación.**

No son considerados datos personales aquellos que no hagan referencia a una persona, por ejemplo una dirección de correo electrónico del tipo info@empresa.com; datos anonimizados y/o disociados, siempre y cuando el proceso de desambiguación del dato no sea reversible.

Finalmente en este punto, queremos realizar una breve aclaración. La Ley de Protección de datos Personales N° 1845, determina al domicilio como dato personal no sensible, conforme lo hemos detallado ut supra.

No obstante ello, debemos poner especial atención sobre este punto debido a que el **domicilio sí debería ser considerado** en la cotidianeidad **como un dato sensible.** Su posible divulgación sugiere un riesgo en la persona: vulnera su intimidad y privacidad, sobre todo en casos de violencia de género.

En ese sentido, reiteramos la importancia del contexto y la finalidad según el ámbito en que se desarrolle o publique un dato.

3.3.2.Datos sensibles

Son aquellos datos personales que tienen un resguardo especial ya que por medio de su conocimiento, la persona podría ser discriminada. Son aquellos que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro **dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio a su titular.**

Sobre lo referido, corresponde resaltar que una clasificación efectiva de los datos, garantizará que la información reciba la protección adecuada de acuerdo con su sensibilidad, valor y **criticidad** (*ver "criticidad del dato"*), así como la naturaleza y el grado de riesgos que resultan de una divulgación indebida, daño o destrucción.

3.3.2.1.Datos de salud

Los datos relativos a la salud constituyen la categoría “datos sensibles” en la normativa vigente, y la ley les impone una protección más rigurosa, estableciendo criterios específicos los cuales se detallarán a continuación:

En principio, el tratamiento de los datos de salud está prohibido, siempre y cuando no exista consentimiento de la persona titular. Pueden existir excepciones, como por ejemplo, el caso de procesamiento y cesión de este tipo de datos por parte de los establecimientos sanitarios y los profesionales de la salud, **en cumplimiento del secreto profesional** aún después de finalizada la relación con el paciente.

En esta misma línea, los ministerios de Salud, tanto a nivel nacional como provincial y de la Ciudad Autónoma de Buenos Aires, se encuentran facultados a requerir, recolectar, cederse entre sí o procesar de cualquier otro modo información de salud sin consentimiento de los pacientes, conforme las competencias explícitas e implícitas que les hayan sido conferidas por ley[1].

Si se tratase de datos personales relativos a la salud de las personas y su tratamiento es necesario por razones de salud pública y emergencia establecidas por autoridad competente y debidamente fundadas, se puede prescindir del consentimiento de los titulares[2].

Para utilizar la información del paciente con fines incompatibles con su tratamiento médico, es necesario su consentimiento pleno, libre e informado[3].

En este sentido, la divulgación del nombre de un paciente que padezca de algún virus estará permitida siempre y cuando hubiese sido requerido su consentimiento, en un contexto pandémico[4].

3.3.3.Datos personales con régimen particular

3.3.3.1.Datos de inteligencia

El tratamiento de datos personales por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia puede efectuarse sin consentimiento de la persona titular de los datos, en aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas, en casos donde la defensa nacional o la seguridad pública se encuentren en peligro o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

[1] Cf. Art. 5°, inc. 2 b), y art. 11°, inc. 3 b) de la Ley N° 25.326.
[2] Cf. Art. 7°, inc. 4 de la Ley N° 1.845 de la Ciudad Autónoma de Buenos Aires.
[3] En este sentido, ver Guía para el tratamiento de los datos personales ante el Coronavirus Covid-19, emitida por la AAIP.
[4] Ibidem.

3.3.3.2.Secreto bancario

Será de aplicación la ley de entidades financieras N° 21.526. Se refiere específicamente a las operaciones pasivas que realicen las entidades financieras.

Las operaciones pasivas tienen como finalidad esencial procurar recursos para que los bancos e instituciones financieras puedan realizar sus inversiones y, por lo tanto, cumplir su función económica. A través de ellas se captan tanto recursos propios (capital y reservas), como recursos ajenos, siendo estos últimos los más importantes.

Algunos ejemplos: captación de ahorro, operaciones interbancarias, cuentas corrientes a la vista, cuentas de ahorro, imposiciones a plazo fijo, depósitos indicados, depósitos estructurados, depósitos asegurados (en general, cualquier tipo de depósito); fondos de inversión, planes de ahorro, pensiones.

padres o sus propios apodos. Esto conduce a la identificación indirecta del niño, niña y adolescente, y debe ser evitado también."[5]

3.3.3.3.Secreto fiscal

Se encuentra regulado en la ley N° 11.683 y el Código Fiscal de la Ciudad Autónoma de Buenos Aires. Es el instituto consagrado para resguardar las documentaciones, manifestaciones y declaraciones (información sensible patrimonial) que presenten y formulen los contribuyentes ante el organismo fiscal.

Al respecto, cabe destacar que el artículo N° 86 del Código Fiscal de la Ciudad Autónoma de Buenos Aires establece algunas excepciones al secreto fiscal referido, los cuales se detallarán en la sección relativa a *cesión de bases de datos*.

3.3.4.Datos referidos a niñeces y adolescencias

Son una subespecie de datos personales, pero que no conforman la categoría de datos sensibles; siempre y cuando no se encuentren en los supuestos mencionados anteriormente.

Sin embargo, las normas le imprimen un resguardo especial, teniendo en cuenta el "interés superior de las niñeces", y ordenan que éste debe ser preservado por encima de cualquier otro interés.

En estos casos, no sólo hay que verificar si es dato sensible o no, sino que también hay que verificar que el tratamiento no afecte el interés superior de las niñeces.

Al respecto, el interés superior de las niñeces posee raigambre constitucional (art. 75, inc. 22). A su vez, se encuentra reconocido en la Convención de los Derechos del Niño y es

[5] https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-4_ProteccionDatos_Interior_WEB.pdf

reproducido por la ley 23.849, la cual establece que ha de entenderse como Interés Superior del Niño, Niña y Adolescente, y la "*máxima satisfacción, integral y simultánea de los derechos y garantías reconocidos en esta ley*", debiéndose respetar, entre otras aristas, lo que se detalla a continuación: *"su condición de sujeto de derecho, el respeto al pleno desarrollo personal de sus derechos en su medio familiar, social y cultural".*

Un ejemplo que brinda el Fondo de las Naciones Unidas para la Infancia (UNICEF) es el siguiente: "*A diario se expone en los medios a chicas y chicos en estado de vulnerabilidad, en conflicto con la ley penal o en situaciones de violencia, invadiendo su intimidad y perjudicando su dignidad. A veces los medios utilizan recursos de edición como el pixelado, el desenfocado o la cobertura del área de los ojos para evitar exponer la identidad de chicos y chicas en sus coberturas periodísticas. Estos recursos suelen ser insuficientes y, por lo tanto, inefectivos. En otras ocasiones, se omiten los datos personales de un niño o niña pero se difunden informaciones que permiten deducir sus identidades, como por ejemplo la escuela a la que asisten, la calle donde viven o los nombres de sus*
Aquí se puede ver cómo la utilización de la información no respeta el interés superior. Sin embargo, si el tratamiento de determinados datos se utiliza para generar una política pública que garantice derechos y dignifique, estamos hablando de imponer su interés superior por sobre todo.

A pesar de lo manifestado, es importante advertir que si se puede alcanzar el mismo resultado disociando la información, esta última técnica es la que debe prevalecer.

3.4.Datos anónimos

Son aquellos a los que se le han aplicado medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona humana sin esfuerzos desproporcionados.

En la misma línea, la Agencia Española de Protección de Datos Personales en su guía "Orientaciones y garantías en los procedimientos de anonimización de datos personales" del año 2016, la define como aquel proceso que tiende a eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos. Además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleve una distorsión de los datos reales. Un análisis masivo de los datos que puedan derivar de los datos anonimizados no debería diferir del análisis que pudiera obtenerse si hubiera sido realizado con datos no anonimizados.

La Ley Nacional N° 25.326 de protección de los datos personales en su artículo N° 2 define a la disociación de datos como *"todo aquel tratamiento donde la información obtenida no pueda asociarse a persona determinada o determinable."*

En tal sentido, la Unión Europea, a través del Reglamento General de Protección de Datos (RGPD), señala que los datos anónimos constituyen "aquella información que no hace referencia a personas naturales identificadas o identificables o a datos personales que se anonimizan de tal forma que dejan de ser identificables". Una anonimización del 100% es el objetivo más deseable desde el punto de vista de la protección de los datos personales. En algunos casos no es posible y debe contemplarse un riesgo residual de reidentificación.

El riesgo residual de reidentificación es la probabilidad de que, a través de técnicas de conversión de los datos, se pueda individualizar a la persona. Esta situación podría darse en los siguientes casos:

- si se desarrollan tecnologías que permitan descifrar la anonimización.
- si algunos datos dejan de ser anónimos.
- si se relacionan datos que no son anónimos y a raíz de eso se puede llegar a la identidad de alguien.

Cualquier proceso sólido de anonimización debe evaluar el riesgo de reidentificación, que debe gestionarse y controlarse a lo largo del tiempo

Cabe mencionar que, el riesgo de reidentificación nunca puede considerarse nulo, pero, en cualquier caso, la anonimización ofrece mayores garantías de privacidad a las personas.

Para profundizar en esta temática,se aconseja la lectura de la "*Guía de Consejos y Recomendaciones para la anonimización de datos personales*", elaborada por la Subsecretaría de Políticas Públicas Basadas en Evidencias, la cual tiene como objetivo ofrecer criterios indicadores y orientadores en el ámbito del Poder Ejecutivo del Gobierno de la Ciudad Autónoma de Buenos Aires sobre buenas prácticas en materia de la anonimización de datos personales.

4. Cesión de datos en el sector público

Habiendo repasado las categorías de datos, y algunos ejemplos de cada uno, corresponde entonces focalizarnos en un punto esencial, la cesión de los mismos.

En esta sección se abordará cómo deben compartirse los datos (ya sean personales o sensibles) entre las diferentes entidades y jurisdicciones de gobierno, y también hacia el sector privado.

El principio general aplicable a todas las categorías de datos es el **consentimiento**. Por ende, previo a cualquier tratamiento o cesión de datos corresponde solicitar el consentimiento de la persona titular del dato y brindarle información clara y precisa respecto al tratamiento y utilización de los mismos.

Sin embargo el artículo N° 10 de la ley N° 1845 establece una excepción al consentimiento y es que la cesión se "realice entre órganos del sector público de la Ciudad de Buenos Aires en forma directa, en la medida del cumplimiento de sus respectivas competencias".

Las distintas dependencias del ámbito público podrán ceder entre sí sus datos personales, en forma directa y **sin el consentimiento del titular de los datos**, en la medida en que sea necesario para el cumplimiento de sus respectivas competencias.

En los supuestos de cesión de datos personales entre organismos públicos de la Ciudad Autónoma de Buenos Aires, se cumple con las condiciones de licitud y no se requiere el consentimiento del titular de los datos, en la medida en que:

(i) El cedente haya obtenido los datos en ejercicio de sus funciones,

(ii) El cesionario utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de su competencia,

(iii) Los datos involucrados sean adecuados y no excedan el límite de lo necesario en relación a esta última finalidad.

Ahora bien, en función de la categorización que analizamos anteriormente podemos determinar en líneas generales que:

1. No hay restricciones para las cesiones de **datos públicos** y **anónimos**. Esto significa que no aplica el art. 10 de la ley 1845 de CABA, y pueden ceder libremente todo este tipo de datos.
2. Respecto a los **datos personales de carácter general**, aplica el art. 10 citado anteriormente, es decir, el consentimiento del titular de los datos no será exigido cuando:
    a. Se realice la cesión de manera directa entre órganos del sector público de CABA en cumplimiento de sus respectivas competencias.
    b. El cedente haya obtenido los datos en ejercicio de sus misiones y funciones.
    c. El cesionario utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de su competencia.
    d. Los datos involucrados sean adecuados y no excedan el límite de lo necesario en relación a esta última finalidad.
3. Los **datos sensibles,** sin consentimiento del titular de los mismos, solo podrán cederse si existen razones de interés general fundadas por ley. Teniendo en cuenta el tipo de datos que se trata en estos casos, como buena práctica, se sugiere la

suscripción de convenios de confidencialidad y no divulgación de la información entre los usuarios involucrados en la cesión y quienes manipularon la información. Por ejemplo: entre la repartición actuante y sus agentes, o entre la repartición actuante y empresas contratistas para el tratamiento o almacenamiento de los datos.

4. Los **datos fiscales** podrán cederse por requerimiento de organismos fiscales nacionales, provinciales y municipales o de autoridad judicial en los procesos criminales por delitos comunes.

4.1. Procedimiento para la cesión de datos entre organismos públicos

La presente guía de clasificación de los datos se crea a los efectos de estandarizar y simplificar la cesión de los mismos entre organismos pertenecientes al sector público, promoviendo en todos los casos el cumplimiento de los estándares propios de seguridad, verificación, control y efectividad de los procesos.

Por ello, en conformidad con los lineamientos establecidos por el Decreto N° 118 de fecha 01 de abril de 2022, por el cual se estableció un modelo de gobernanza de los datos, y por la Resolución N°136 de fecha 10 de junio de 2022 de la Secretaría de Innovación y Transformación Digital, se definen los siguientes lineamientos:

4.1.1. Procedimiento en función del tipo de dato:

4.1.1.1. Datos de acceso público irrestricto:

Las entidades y jurisdicciones del Poder Ejecutivo que cuenten con datos de fuentes de acceso público irrestricto deberán disponibilizarlos sin ningún requisito previo.

El cedente deberá efectuar las acciones necesarias a los fines de realizar la cesión solicitada. De considerarlo necesario, podrá requerir la asistencia técnica de la Secretaría de Innovación y Transformación Digital.

4.1.1.2. Datos públicos:

Para la cesión de los mismos no se requiere acreditar derecho subjetivo, ni tampoco cumplimentar ningún protocolo específico.

La solicitud para el acceso a las bases de datos públicas deberá realizarse conforme lo establecido en el artículo N° 9 de la Ley N° 104, pudiendo ser presentada por medio escrito o por vía electrónica, y no estará sujeta a ninguna otra formalidad.

Las entidades y jurisdicciones del Poder Ejecutivo no pueden negarse a brindar dicha información, efectuando todas las acciones necesarias para realizar la cesión solicitada.

4.1.1.3 Datos personales:

La cesión de datos personales entre entidades y jurisdicciones del Poder Ejecutivo, en el

marco de sus respectivas competencias, se deberá efectuar a través de un medio informático auditable que permita acceder a la finalidad de la cesión, las competencias y funciones de cada parte, el tipo de dato y su fuente.

Para ello, las reparticiones cesionarias deberán utilizar el *"Modelo de Requerimiento para la Cesión de Datos"* creado por la **Resolución N°136-SECITD/22,** enviándolo a la repartición cedente mediante el módulo de Comunicaciones Oficiales del sistema SADE, el cual se adjunta a la presente Guía como Anexo lll.

Por otro lado, en caso que los datos personales a ceder sean sensibles, conforme lo establecido en la Ley N° 1.845 de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires deberá existir consentimiento previo, libre, expreso e informado de la persona titular de los datos, a la que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo, salvo que existan razones de interés general fundadas por ley.

En caso que la información referida a datos personales que se pretenda ceder haya sido previamente sometida a un proceso de anonimización o disociación de los datos, no será necesario dar cumplimiento a los requisitos de los párrafos precedentes.

4.1.2. Obligaciones y deberes de las reparticiones

Las entidades y jurisdicciones deberán procurar que los datos susceptibles de cesión cuenten con las medidas específicas de seguridad según su clasificación, en función de las normas que regulan la materia, siendo las responsables de velar por la exactitud, completitud, consistencia, credibilidad, pertinencia, integridad y actualidad de sus datos.

Por otro lado, al momento de utilizar el *modelo de requerimiento para la cesión de datos* creado por Resolución N°136-SECITD/22, ut supra referido, declaran ajustarse a los siguientes puntos:

- Conocer y dar cumplimiento a lo establecido en Ley Nacional N° 25.326 y la Ley N° 1.845 de Protección de los Datos Personales, sus normas reglamentarias, y demás normativas complementarias y vigentes en la materia.

- Conocer que los datos personales objeto de tratamiento sólo pueden ser cedidos en los términos del artículo 10 de la Ley N° 1.845.

- Declarar que todos los datos que se solicitan serán tratados en el marco de las competencias conferidas por el Decreto N° 463/19 y sus modificatorios, y conforme lo establecido en la Ley Nacional N° 25.326 y la Ley local N° 1.845, sus normas reglamentarias, complementarias y demás normativas vigentes en la materia.

5. CESIÓN DE DATOS AL SECTOR PRIVADO

Los organismos públicos podrán ceder los datos personales **no sensibles** en su poder al sector privado **de manera no masiva**, siempre que dicha cesión se realice con motivo del

ejercicio de las funciones propias del organismo o en virtud de una obligación legal, y cuando se encuentre justificado en el cumplimiento del requisito del interés legítimo. Asimismo, el organismo deberá asegurarse que con dicha cesión no se ocasione ningún perjuicio a las personas titulares de los datos.

Además, el organismo público deberá verificar que el cesionario sea capaz de dar cumplimiento a los principios de protección de datos que resulten aplicables al caso.

La cesión masiva de datos personales de bases de datos públicas a registros privados **sólo puede ser autorizada por ley o por decisión de autoridad funcionaria responsable**, bajo el cumplimiento de los siguientes requisitos:

- Los datos motivo de la cesión son de acceso público.
- Fue garantizado el respeto a los principios de protección de datos personales.
- Dicha cesión no ocasiona perjuicio alguno a las personas titulares de los datos.

Anexo I

A continuación se desarrollarán algunos ejemplos prácticos donde se podrán observar los procedimientos para la cesión de datos públicos y personales, en función del contenido expuesto en esta guía.

a. Pedidos en el marco de la Ley N° 104

Pueden ser transferidos y comunicados a cualquier persona humana o jurídica que los solicite. El Gobierno de la Ciudad Autónoma de Buenos Aires, tiene la obligación legal de proporcionarlos.

Ejemplos prácticos de pedidos de información: Una empresa periodística envía un pedido de información en el marco de la Ley N° 104, solicitando nombre y apellido, enfermedades laborales y adhesión sindical de las personas funcionarias de su área. ¿Qué hacer? En este caso, se deberá dar respuesta al pedido de información por obligación legal, pero **no deberemos detallar todos los datos solicitados**. Los únicos que podremos informar serán **nombres y apellidos** ya que, al figurar en registros públicos estatales por pertenecer a la dotación de la repartición consultada, estos datos son considerados públicos.

Los datos correspondientes a la salud y afiliación a sindicato no pueden transferirse por ser **sensibles**.Esos datos sí se podrían compartir si, por ejemplo, **se pide el porcentaje total de personas funcionarias afiliadas a sindicatos, o algún otro dato anónimo.** Al no revelarse la identidad de las personas, no habría inconveniente.

b. Pedido de información entre áreas gubernamentales.

La Dirección General Competencias Comunales y Talleres, perteneciente a Jefatura de Gabinete de Ministros, requiere al Ministerio de Justicia y Seguridad un reporte de las denuncias por comisión de delitos ingresadas en el 2021, donde deberán detallarse los

datos personales de las personas denunciantes y denunciadas. En este sentido, una de las competencias de la Dirección General referida, establecidas mediante el Decreto de estructura N° 463/19, es la de “coordinar con el Ministerio Público Fiscal y el Ministerio de Justicia y Seguridad los procedimientos a seguir cuando existan denuncias por comisión de delitos.”

Es por ello que los datos podrán ser compartidos **sin consentimiento previo** del titular, en virtud de los parámetros establecidos en el artículo N° 10 de la ley N° 1.845, el cual establece una excepción al consentimiento: la cesión se realizaría “ entre órganos del sector público de la Ciudad de Buenos Aires en forma directa, **en la medida del cumplimiento de sus respectivas competencias”.**

Anexo II

Teoría sobre la clasificación de datos

Las siguientes formas de clasificación de datos sirven para comprender mejor cada activo. Pueden entenderse por separado pero sin embargo su interconexión es lo que agrega valor.

Para el año 2004, el gobierno de la República Argentina comenzó a delinear los requisitos para formar e implementar una estrategia nacional de protección de datos que abarcó la creación de un **modelo de política de seguridad** que designa las mejores prácticas para la protección y gestión de datos como parte de su gestión de riesgos.

Los organismos públicos y privados fuente de datos son responsables de su clasificación, en función del grado de sensibilidad, documentación y actualización.

Dentro de la clasificación, la política debe basarse en los siguientes tres factores: **confidencialidad, integridad y disponibilidad**. Cada uno de los tres factores tiene una escala de 0 a 3, que luego determina el grado de protección que debe recibir. La escala en la que se divide es la siguiente:

- **Baja criticidad:** La información se clasifica como pública. Es comúnmente conocida y utilizada por cualquier persona o empleado. Una modificación no autorizada puede repararse fácilmente y no compromete las operaciones de la organización.
- **Criticidad media:** La información se clasifica como reservada o para uso interno. Puede ser conocida o utilizada por algunos empleados de la organización y algunas autoridades delegadas externas. Su uso podría causar leves riesgos o pérdidas para la agencia, el sector público nacional o terceros. Una modificación no autorizada podría repararse, aunque podría causar ligeras pérdidas para la agencia pública o terceros asociados. Su pérdida de un día o permanente podría causar daños significativos a las operaciones en la organización.

- **Alta criticidad:** La información se clasifica como confidencial o secreta. Ésta sólo puede ser conocida por un grupo de empleados, generalmente la alta dirección de la organización, y su divulgación o uso no autorizado podría causar serias pérdidas al sector público u otros terceros asociados. La pérdida permanente podría causar graves daños a la organización.

Anexo III

Modelo de convenio de confidencialidad

Se deja expresa constancia que el modelo desarrollado a continuación obedece a criterios mínimos de cumplimiento, pudiendo la repartición actuante agregar contenido pertinente y adaptar a cada caso de uso particular el texto en cuestión.

ACUERDO DE CONFIDENCIALIDAD

Y NO DIVULGACIÓN DE LA INFORMACIÓN

En virtud de los servicios prestados a la xxxxxxxx (en adelante, la Repartición), quien suscribe ..... (nombre y apellido), DNI N° ....., declaro conocer que los datos a los que tengo acceso en virtud de las tareas desempeñadas, se encuentran amparados bajo normas de confidencialidad indicadas a continuación.

El presente acuerdo se ajusta a lo mentado por la Ley de la Ciudad Autónoma de Buenos Aires N° 1.845 de Protección de Datos Personales, su Decreto Reglamentario N° 725/2007, y toda aquella normativa concordante y relacionada, como también aquellas que en el futuro la sustituyan, amplíen, modifiquen y/o regulen. Al respecto, quien suscribe declara conocer el contenido de dichas normas.

Quien suscribe se obliga de forma irrevocable a no revelar, divulgar o transmitir, ceder, ni facilitar de cualquier forma o por cualquier medio, ya sea por acción u omisión, a toda persona humana o jurídica, y a no utilizar para su propio beneficio o de cualquier otra persona, humana o jurídica, cualquier información, dato, o documentación a la que acceda o sobre la que tenga conocimiento como consecuencia de la prestación del servicio referido en el párrafo anterior.

Dentro de esta obligación también se incluye cualquier información, dato o documentación de terceras partes o personas a la que hubiese accedido o tenido conocimiento en la prestación del referido servicio, y la administración de los datos almacenados o transferidos a la presente Repartición, o sobre los que la referida Repartición hubiese actuado de intermediaria. La enunciación precedente no tiene carácter taxativo. Ante la duda prevalecerá el carácter confidencial de la información, dato o documentación.

Quien suscribe declara conocer que la obligación de confidencialidad, reserva y no divulgación de la información se extiende a todas las personas integrantes de la Repartición, sin importar el modo de vinculación con ésta.

En consecuencia, quien suscribe, se compromete a realizar las acciones debajo previstas, sin perjuicio de aquellas otras obligaciones que le correspondan por ley. La siguiente enumeración no es taxativa:

1. Guardar la máxima reserva y secreto sobre la Información Confidencial en los términos del presente Acuerdo;
2. Utilizar la Información Confidencial únicamente para la prestación de los servicios prestados a la repartición. Todo otro uso distinto al aquí dispuesto deberá contar con el expreso consentimiento de autoridad competente.
3. No reproducir por ningún medio la Información Confidencial, excepto en la exacta medida en que ello resulte necesario para la prestación de los servicios a la repartición, y siempre que dicha reproducción no implique poner la Información Confidencial al alcance de terceros.
4. No divulgar, proporcionar, o revelar a terceros, en cualquier forma, la Información Confidencial.
5. Restituir toda la Información Confidencial al solo requerimiento de la Repartición.
6. Observar y adoptar cuantas medidas de seguridad sean necesarias para asegurar la confidencialidad, secreto e integridad de la Información Confidencial.
7. Observar y adoptar las medidas necesarias para garantizar la debida Protección de los Datos Personales.
8. Observar todas las políticas de seguridad implementadas por la Repartición con respecto a la Información Confidencial y la Agencia de Seguridad Informática (ASI).
9. A reconocer la propiedad intelectual y transferir, en favor de la Repartición, todo trabajo y/o proyecto; desarrollo; conocimiento; producido; desarrollado y/o proyectado, por quien suscribe en el marco y transcurso de la prestación de sus servicios.

Esta obligación de confidencialidad, reserva y no divulgación de la información subsistirá sin vencimiento de plazo, aún después de finalizada la prestación de los servicios a la Repartición, asumiendo la responsabilidad penal, administrativa y/o civil de los daños y perjuicios que por dolo y/o negligencia pudiera ocasionar la violación de los términos mencionados en el presente Acuerdo.

En....., a los.....días del mes de.....de 20.....-

Anexo IV

Términos y Condiciones Generales de Uso de Datos Personales

Se deja expresa constancia que el modelo desarrollado a continuación obedece a criterios mínimos de cumplimiento, pudiendo la repartición actuante agregar contenido pertinente y adaptar a cada caso de uso particular el texto en cuestión.

INTRODUCCIÓN

Los presentes términos y condiciones de uso e información legal (en adelante, Términos y Condiciones) aplican para la plataforma _____ (en adelante, la plataforma) y no así, para el uso de otras aplicaciones móviles o portales web del GCABA que pudieran surgir con posterioridad, y resultan independientes de cualquier responsabilidad que pueda surgir del uso de los mencionados servicios.

La plataforma es administrada y controlada por la _____ (Ministerio, Secretaría, Subsecretaría, Dirección General), perteneciente al poder ejecutivo del Gobierno de La Ciudad Autónoma de Buenos Aires, en adelante "el GCABA", en uso de las funciones y misiones conferidas por Decreto N° 463 de fecha 13 de diciembre de 2019, entre las cuales se encuentran: _____

Al acceder o utilizar cualquier parte de la plataforma, la persona usuaria estará aceptando los Términos aquí reseñados.

DEFINICIONES

1. Persona usuaria: cualquier persona humana que accede a la plataforma.
2. *Agregar demás aplicativos que tenga la plataforma, por ejemplo Login, Validación de identidad, buzón de notificaciones, etc.*

PERSONAS USUARIAS

Podrán utilizar la plataforma las personas humanas con capacidad para contratar. Las personas menores de edad, de conformidad con la normativa vigente en materia de protección de datos personales, podrán operar mediante autorización expresa de sus representantes legales, bajo su absoluta responsabilidad.

El GCABA podrá solicitar a la persona usuaria para acreditar los puntos anteriormente señalados, toda documentación que estime corresponder a los fines de constatar su identidad, supeditando tal cumplimiento, al uso de la plataforma.

CONSENTIMIENTO

A través de la aceptación de los presentes términos y condiciones, la persona titular de los datos personales presta expreso consentimiento, conforme lo referido por la Ley de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires, N° 1.845, para que, el GCABA, o terceras partes designadas por éste, tengan derecho de acceso y tratamiento, a los mismos.

El consentimiento podrá ser revocado por cualquier medio y en cualquier momento y sin necesidad de justificar el motivo por parte de la persona usuaria. Dicha revocación no tendrá efectos retroactivos.

DERECHOS Y OBLIGACIONES DE LAS PERSONAS USUARIAS

El GCABA pondrá a disposición, todas las herramientas necesarias para que las personas usuarias, en su calidad de titulares de sus datos puedan ejercer los derechos reconocidos en el art. 13 de la Ley N° 1845, a saber: acceso, rectificación, actualización, pedido de confidencialidad o supresión.

Los derechos referidos, podrán ser solicitados enviando el requerimiento a la casilla de correo _____ o en forma presencial en las oficinas ubicadas en _____ Ciudad Autónoma de Buenos Aires, de lunes a viernes de 09:00 a 17:00hs.

La persona usuaria, titular de los datos, podrá ejercer los derechos mencionados por sí o a través de sus representantes legales o convencionales. Se encuentran facultados del mismo modo los sucesores de las personas humanas.

Asimismo, conforme lo referido en Artículo N° 15 de la Ley N° 1845, el GCABA puede denegar el acceso, rectificación, actualización, pedido de confidencialidad o supresión solicitada por el titular del dato, en función del orden o la seguridad pública, o de la protección de los derechos o intereses de terceros cuando así lo disponga una autoridad judicial a partir de una medida cautelar inscrita.

Por otra parte, la persona usuaria deberá:

(a) proveer información verdadera, correcta, actual y completa acerca de su persona en función de lo requerido en el formulario de registro , y

(b) mantener y actualizar en todo momento los Datos de Login a fin de conservarlos veraces, correctos, actuales y completos. Si suministra información que es falsa, inexacta, desactualizada o incompleta, o si existen indicios razonables para sospechar que dicha información es falsa, inexacta, desactualizada o incompleta, miBA tendrá el derecho de suspender o cerrar su cuenta y negarle el uso presente o futuro del Servicio (o cualquier parte del mismo). Sin perjuicio de las acciones administrativas o judiciales que pudieran corresponder.

RECOLECCIÓN DE DATOS

Los dato serán recopilados de la siguiente manera ____

OBJETO DE LA RECOLECCIÓN

La información que se obtenga de la persona usuaria, tendrá como finalidad _____ y/o cualquier otra funcionalidad que se incorpore a futuro.

ALMACENAMIENTO DE LOS DATOS

Los datos se almacenarán en la base de datos creada por la autoridad competente, según lo estipulado en el art. 4° de la Ley de Protección de Datos Personales N° 1845 de la Ciudad Autónoma de Buenos Aires.

Asimismo se hace saber que los datos recopilados podrán ser almacenados en servidores propios del GCBA o en la nube, pudiendo o no, encontrarse dentro de las regiones adecuadas mencionadas en la Disposición N° 60 de la Dirección Nacional de Protección de Datos Personales, de fecha 18 de noviembre de 2016.

CADUCIDAD DE ALMACENAMIENTO DE LOS DATOS

Los datos brindados por la persona usuaria se almacenarán por un plazo perentorio de _____

Transcurrido ese tiempo, se procederá a disociar los datos identificatorios recabados, persistiendo en las bases de datos del GCABA únicamente información agregada.

Por otra parte, se deja expresamente señalado que en situaciones excepcionales, se podrá conservar toda la información obtenida, durante un período extendido, según: el mérito, oportunidad y conveniencia que considere la administración; que la misma esté sujeta a un requisito u obligación legal; investigación gubernamental o relacionadas con posibles incumplimientos; para evitar daños y perjuicios.

POLÍTICA DE PRIVACIDAD

El GCABA respeta la privacidad de las personas usuarias y garantiza la protección de sus datos.

El GCABA no pedirá ni agregará ningún dato sensible sin el expreso consentimiento de la persona usuaria en conformidad con los parámetros establecidos por Ley N° 1.845 (Texto Consolidado por Ley N° 6.347), Decreto N° 1501/09, Ley Nacional de Protección de Datos Personales N° 25.326 en conjunto con su Decreto Reglamentario N° 1558/2001 y las reglamentaciones que sus respectivas autoridades de aplicación dispongan.

El GCABA, además de cumplir con la normativa vigente en materia de medidas de seguridad aplicable al tratamiento de datos personales, adicionalmente utilizará los

estándares de la industria en materia de protección de la confidencialidad de los mismos.

Sin embargo, el GCABA no se responsabiliza por interceptaciones ilegales de los dispositivos móviles que utilicen las personas usuarias, que puedan afectar la seguridad de la información almacenada en el mismo, por parte de terceros no autorizados.

Finalmente, se hace saber que los datos podrán ser obtenidos, almacenados o procesados por terceros, en el marco de lo referido en el art. 5° de la ley 1845 de CABA,

Los contratos de prestación de servicios de tratamiento de datos personales por terceros, contendrán los niveles de seguridad exigidos por la normativa vigente, así como también las obligaciones relativas a la confidencialidad y reserva que deben mantener sobre la información obtenida, a los fines de evitar una disminución en el nivel de protección de los datos personales.

ENLACES DE TERCERAS PARTES

Cierto contenido disponible en la plataforma puede incluir material de terceras partes, se advierte que el Gobierno de La Ciudad Autónoma de Buenos Aires no administra ni controla estos sitios y no será responsable de sus contenidos ni de cualquier daño o perjuicio causado por tales contenidos, productos o servicios disponibles en dichos sitios.

El GCABA no es responsable de cualquier daño o perjuicio relacionados con la adquisición o utilización de bienes, servicios, recursos, contenidos, o cualquier otra transacción realizada en conexión con sitios web de terceros. La persona usuaria debe revisar cuidadosamente las políticas y prácticas de terceros y asegurarse de entenderlas antes de participar en cualquier transacción. Quejas, reclamos, inquietudes o preguntas con respecto a productos de terceros deben ser dirigidas a la tercera parte.

El GCABA no será responsable ni garantizará el cumplimiento de las obligaciones que hubiese asumido la persona usuaria en las diferentes aplicaciones que no sean parte de la plataforma del sitio bajo análisis o que surjan implícitamente, en relación a los pagos a efectuar y/o recibir,en cuanto a la prestación de los servicios publicados y/o cualquier otro tipo de responsabilidad que pueda surgir ligada a la utilización de las plataformas a las cuales se acceda a través del sitio.

PROPIEDAD INTELECTUAL

Las imágenes, marcas, avisos, nombres comerciales, frases de propaganda, dibujos, diseños, logotipos, textos, etc. que aparecen en en el sitio son propiedad del GCABA, excepto cuando se aclare. El GCABA se reserva todos los derechos sobre la plataforma y el contenido de la misma, no cede ni transfiere a favor de la persona usuaria ningún derecho sobre su propiedad intelectual.

DIVULGACIÓN E INTERCAMBIO DE INFORMACIÓN

El GCBA podrá suministrar la información personal de la persona usuaria a terceros, en caso de ser requerido por las autoridades judiciales y cualquier otra exigencia legal que corresponda.

CAMBIOS EN LOS TÉRMINOS Y CONDICIONES

El GCABA podrá modificar estos términos y condiciones ocasionalmente, de manera que recomendamos revisar periódicamente la plataforma, para su revisión y conocimiento.

Si las modificaciones que eventualmente se realicen a estos términos pudieran afectar derechos que la normativa aplicable le reconoce a las personas titulares de los datos personales, los cambios le serán notificados para requerir que presten su consentimiento expreso.

LEGISLACIÓN Y JURISDICCIÓN APLICABLE

Las presentes Términos y Condiciones se rigen en todos sus puntos por las leyes vigentes en la materia en el ámbito de la Ciudad Autónoma de Buenos Aires.

Cualquier controversia derivada de su existencia, validez, interpretación, alcance o cumplimiento, será sometida a los Tribunales en lo Contencioso, Administrativo y Tributario de la Ciudad Autónoma de Buenos Aires.

Asimismo, si un tribunal de jurisdicción competente considera que alguna cláusula o disposición de estos Términos y Condiciones es inválida, ello no afectará a la validez de las restantes cláusulas o disposiciones que permanecerán en pleno vigor y efecto.

Anexo V

Modelo de Requerimiento de Cesión de Datos

Aprobado por Resolución N° 136-SECITD/22

_____ (nombre de la repartición), con domicilio en_____ representado en este acto por _____(nombre y apellido) en su carácter de _____ (cargo), en adelante “LA REPARTICIÓN”, solicita la cesión del siguiente dato, archivo, registro, base o banco de datos_____(completar sólo con la denominación/identificación del dato, archivo, registro, base o banco de datos o similar, que contiene el dato/conjunto de datos a ceder) la cual persiste bajo su órbita.

En tal sentido, conforme las responsabilidades primarias conferidas por Decreto N° 463/19 y sus modificatorios, se encuentran las siguientes:

_____(señalar aquellas que justifiquen la solicitud del dato, archivo, registro, base o banco de datos o similar a ser cedido).

DECLARACIÓN:

● Declaro conocer los lineamientos del Protocolo para la Cesión de Datos del Gobierno de la Ciudad Autónoma de Buenos Aires, aprobado en el marco del Decreto N° 118/22, que se encuentra bajo la órbita de la Secretaría de Innovación y Transformación Digital dependiente de la Jefatura de Gabinete de Ministros, o el organismo que en el futuro la reemplace.

● Declaro conocer y dar cumplimiento a lo establecido en Ley Nacional N° 25.326 y la Ley N° 1.845 de Protección de los Datos Personales, sus normas reglamentarias, demás normativa complementaria y vigente en la materia.

● Declaro conocer que los datos personales objeto de tratamiento sólo pueden ser cedidos en los términos del artículo 10 de la Ley N° 1.845.

● Declaro que todos los datos que se solicitan, serán tratados en el marco de las competencias conferidas por el Decreto N° 463/19 y sus modificatorios, y conforme lo establecido en la Ley Nacional N° 25.326 y la Ley local N° 1.845, sus normas reglamentarias, complementarias y demás normativa vigente en la materia.

Nota: de ser necesario, el cesionario/cedente podrán establecer las necesidades/requerimientos para la cesión, teniendo en consideración la particularidad del dato, archivo, registro, base o banco de datos o similar a ser cedido. Ej. modo, periodicidad, etc.

6. Contacto

Ante cualquier duda o comentario sobre este documento podés escribirnos a **datosgcba@buenosaires.gob.ar**