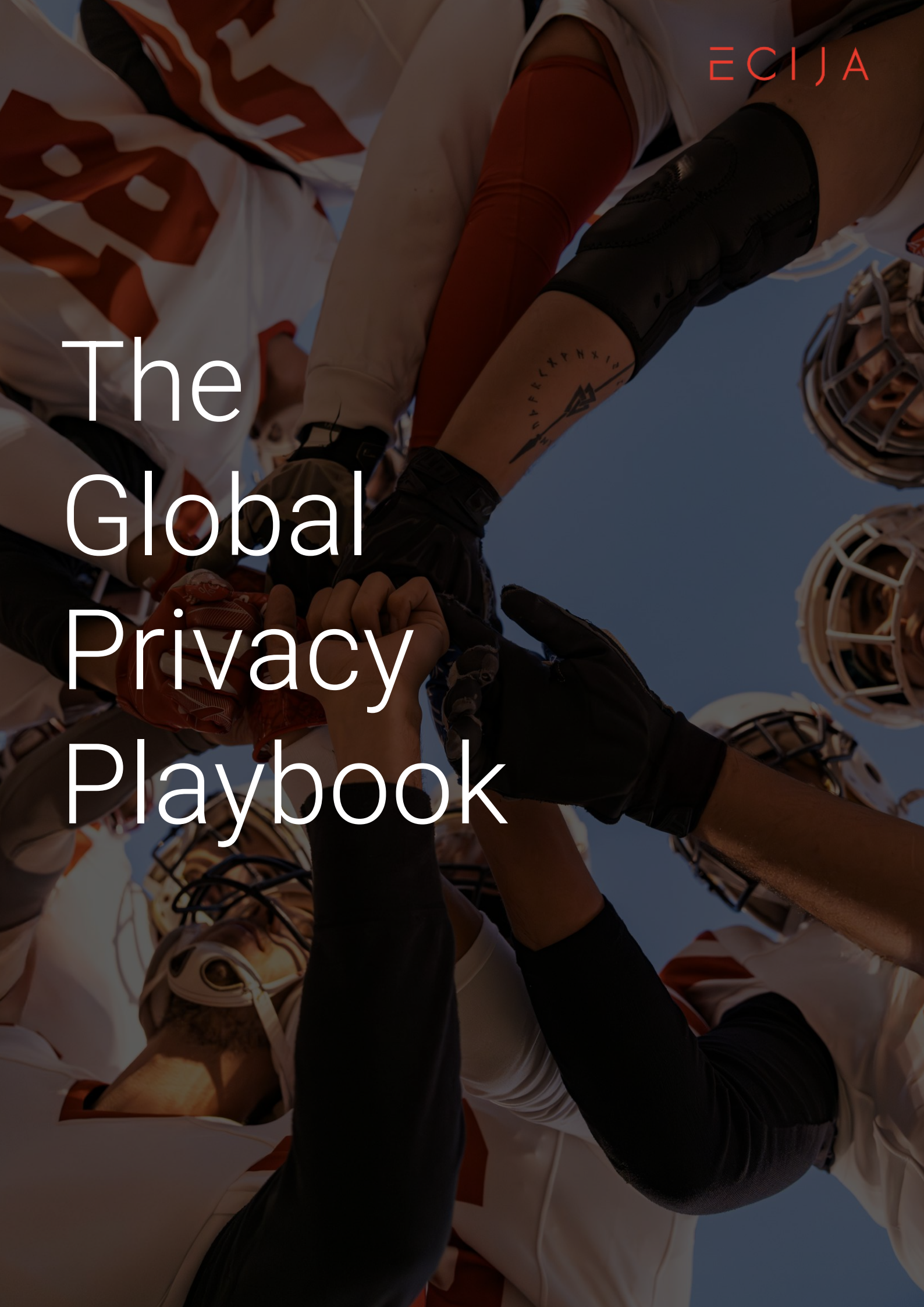
ECIJA

The Global Privacy Playbook



ECIJA

Analizamos de forma comparada los principales marcos normativos en materia de protección de datos personales, abordando derechos de los titulares, obligaciones de las organizaciones, estándares de cumplimiento y enfoques regulatorios a nivel internacional.

Índice

Introducción

La protección de datos personales se ha consolidado como un eje estratégico para las organizaciones que operan en entornos cada vez más digitales, regulados y en constante transformación. En Iberoamérica, este desafío se intensifica ante la coexistencia de marcos normativos en evolución, con distintos niveles de madurez regulatoria y exigencias de cumplimiento.

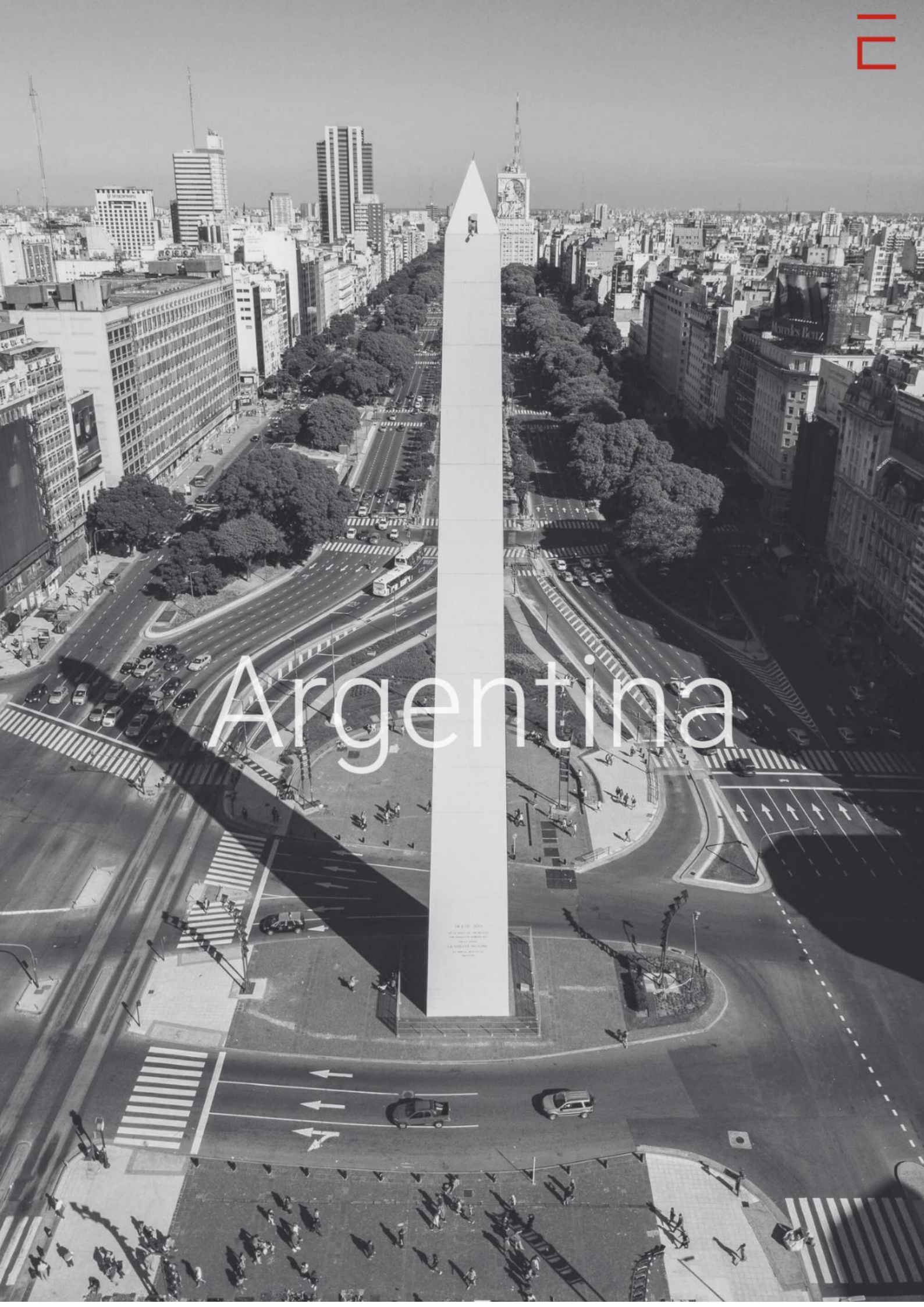
Con el objetivo de ofrecer una visión clara, práctica y regional, se realiza nuestro *Global Privacy Playbook* que reúne las guías comparativas desarrolladas por las distintas oficinas de ECIJA. En este documento, se acompaña un análisis sistematizado de la normativa aplicable en cada una de las jurisdicciones, los principales deberes y obligaciones de cumplimiento de las organizaciones, los derechos de los titulares y los estándares de cumplimiento aplicables en cada país. De esa forma, el Dossier se estructura sobre la base de una metodología común y organizada en torno a preguntas transversales que permiten una lectura clara, ordenada y comparable de cada uno de los marcos normativos.

Sobre el equipo ECIJA

- En ECIJA contamos con un equipo multidisciplinario dedicado exclusivamente a la protección de datos personales y demás áreas de práctica especializadas en tecnología.

- Nuestra presencia internacional, unida a una estrecha colaboración entre las oficinas, nos permite ofrecer soluciones integrales y consistentes tanto a organizaciones locales como multinacionales que operan en múltiples mercados.

- Nuestra trayectoria en el área de protección de datos personales incluye la elaboración e implementación de programas de cumplimiento, la defensa en procedimientos sancionatorios ante las respectivas autoridades de protección de datos de cada país y la adaptación de modelos corporativos a los estándares normativos de cada jurisdicción.


Argentina

- La Ley N° 25.326 regula los principios aplicables, en materia de protección de datos, a aquella información que se encuentra asentada en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos. Además, la Constitución Nacional de Argentina contempla la acción de Habeas Data en su artículo 43, la cual se encuentra destinada a proteger el derecho a la información y a la autodeterminación informativa.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos de información, acceso, rectificación, actualización y supresión. El responsable deberá suministrar la información en forma clara, exenta de codificaciones y en un lenguaje accesible al conocimiento medio de la población.

¿Qué deberes tiene la empresa?

- El responsable deberá cumplir con la obligación de confidencialidad en cada instancia del proceso del tratamiento de datos personales. Además, deberá adoptar medidas técnicas y organizativas acordes para garantizar la seguridad e integridad de la información. Por último, deberán proveer de la información expresa y clara a los titulares acerca de la finalidad de los datos recogidos.

¿Cómo se deben tratar los datos sensibles?

- Podrán tratarse únicamente en el caso de que el titular ha dado su consentimiento para ello. Como excepción, podrán tratarse en la medida en que fueran necesarios para salvaguardar el interés vital del titular, sean tratamientos efectuados por establecimientos sanitarios, sean actividades fundacionales, se requieran para acciones judiciales, para cumplimiento de una obligación laboral y de seguridad, en marco de una asistencia humanitaria o para el ejercicio de las labores estatales.

Encargados de tratamiento de datos personales

- La realización de tratamientos por encargo debe regularse por medio de un contrato entre el encargado y el responsable el cual determinará las instrucciones y las obligaciones que le incumben a cada una de las partes.

¿Se debe contar con un registro de actividades de tratamiento (“RAT”)?

- No se determina como obligación contar con un RAT, pero sí se recomienda realizarlo en vistas a cumplir con las buenas prácticas internacionales. Por su parte, la Ley N° 25.326 establece la obligación de inscribir los archivos, registros, bases o bancos de datos personales ante la Agencia de Acceso a la Información Pública (“AAIP”).

Notificación de incidentes de seguridad

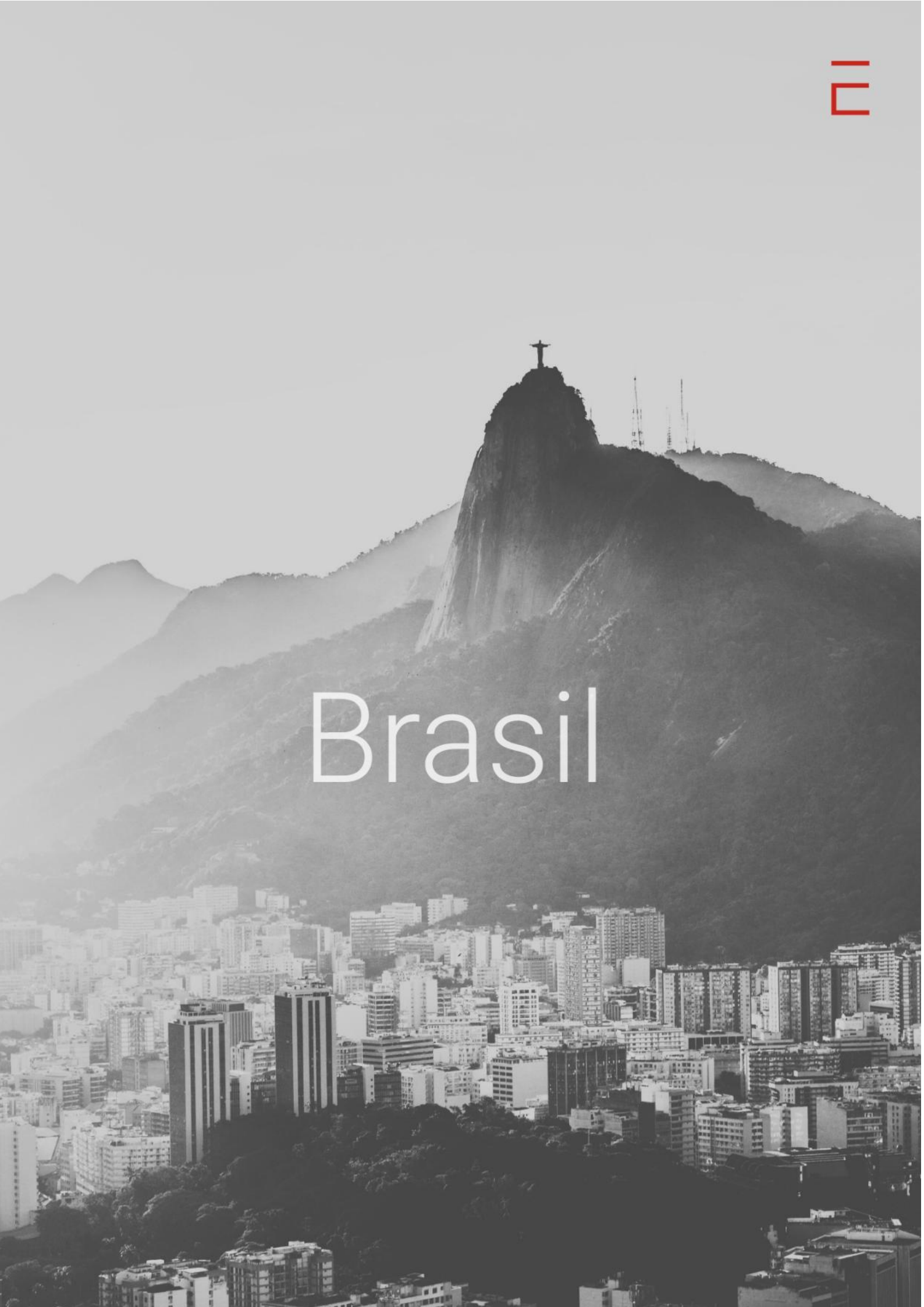
- No existe una obligación legal de notificar los incidentes de seguridad. Sin embargo, ante su ocurrencia, se recomienda notificar a la AAIP y a los titulares de los datos de acuerdo con los lineamientos de la Resolución N° 47/2018 de la AAIP, y actuar conforme a los principios generales de buena fe y prevención del daño del Código Civil y Comercial de la nación.

Evaluaciones de impacto en el tratamiento de datos personales ("EIPD")

- Si bien no han sido receptadas con carácter obligatorio en las normativas, la AAIP emitió la Guía de Evaluación de Impacto en el Tratamiento de Datos Personales con lineamientos que contienen buenas prácticas reconocidas a nivel internacional.

Multas por incumplimiento:

En Argentina las multas por incumplimiento son de carácter penal y administrativo de acuerdo con la gravedad y extensión del incumplimiento legal. En este último ámbito, podrán existir multas de montos graduables hasta la clausura o cancelación del banco de datos.


Brasil

Brasil en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley N° 13.709/2018 regula la recopilación, uso, almacenamiento y protección de los datos personales en Brasil. Además, la Constitución de la República Federativa de Brasil consagra como derecho fundamental la intimidad, vida privada, honor e imagen de las personas.

¿Cuáles son los derechos de los titulares?

- Existen los derechos básicos de información, acceso, rectificación, bloqueo, portabilidad, eliminación y a obtener información por parte de las entidades, tanto públicas como privadas, con las que se compartieron los datos.

¿Qué deberes tiene la empresa?

- Responsabilidad proactiva por medio de la cual se buscará garantizar la seguridad, transparencia y un uso legítimo de los datos personales en todos los tratamientos que efectúe.

¿Cómo se deben tratar los datos sensibles?

- Los datos sensibles sólo pueden tratarse con el consentimiento específico del titular o su representante. Sin embargo, existen excepciones como el cumplimiento de una obligación legal, la ejecución de políticas públicas, la realización de estudios, el ejercicio de derechos, la protección de la vida, o la salud y prevención del fraude.

Encargados de tratamiento de datos personales

- El tratamiento podrá efectuarse por un operador de acuerdo con las indicaciones entregadas por el responsable, quien verificará el cumplimiento de estas instrucciones y de la normativa aplicable.

¿Se debe contar con un registro de actividades de tratamiento?

- Tanto el controlador como el operador deberán llevar un registro de todas aquellas actividades en que se vean involucrados datos personales, con una especial consideración respecto aquellas que se basan en el interés legítimo.

Notificación de incidentes de seguridad

- Los incidentes de seguridad que afecten datos personales deben notificarse a la Agencia Nacional de Protección de Datos y a los titulares en aquellos casos en que exista un riesgo o daño relevante.

Evaluaciones de impacto en el tratamiento de datos personales

- El responsable deberá realizar EIPD de todos aquellos tratamientos que impliquen un alto riesgo para los derechos de los titulares de datos. En esta evaluación se deberá detallar las medidas, salvaguardas y mecanismos de mitigación de riesgos que se aplicarán.

Multas por incumplimiento:

En Brasil las multas por incumplimiento son de hasta 50 millones de reales por infracción (~USD 10 millones) e/o incluso existe la posibilidad de imponer un bloqueo o eliminación de los datos personales relacionados.

Chile

Chile en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley N° 19.628, modificada por la Ley N° 21.719, regula la forma y condiciones en la cual se efectúa el tratamiento y protección de datos personales de conformidad al artículo 19 N° 4 de la Constitución Política de la República, el cual garantiza el respeto y protección a la vida privada y a los datos personales.

¿Cuáles son los derechos de los titulares?

- Los titulares tienen derecho a los denominados derechos BARSOP: Bloqueo, Acceso, Rectificación, Supresión, Oposición y Portabilidad. El responsable de datos debe implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos de forma expedita, ágil y eficaz.

¿Qué deberes tiene la empresa?

- El responsable deberá adecuar su tratamiento a los estándares y obligaciones determinadas en la normativa. Junto a ello, se reconoce el deber de secreto, información y transparencia, protección desde el diseño y por defecto, de adoptar medidas de seguridad apropiadas y de reportar las vulneraciones.

¿Cómo se deben tratar los datos sensibles?

- Sólo pueden tratarse con el consentimiento expreso del titular el cual debe ser otorgado de forma escrita, verbal o por medios tecnológicos. Existen otras excepciones para el tratamiento de esta categoría de datos, como es que sean datos públicos, sean actividades realizadas por una entidad sin fines de lucro, sean para salvaguardar la vida del titular, para formular una defensa jurídica, o bien, en cumplimiento de una obligación legal o cuando ésta así lo mandate.

Encargados de tratamiento de datos personales

- El tratamiento se puede realizar por medio de un tercero mandatario conforme a las instrucciones que se le impartan. Para ello, se debe celebrar un contrato en el que se establecerá el objeto del encargo, su duración, finalidad, el tipo de datos tratados, las categorías de los titulares y los derechos y obligaciones de las partes.

¿Se debe contar con un registro de actividades de tratamiento?

- No es obligatorio contar con un RAT. Sin embargo, en caso de que se elabore un Modelo de Prevención de Infracciones, es necesario identificar aquellas actividades o procesos en que se puede generar o incrementar un riesgo de comisión de infracciones. Sin embargo, se recomienda siempre elaborar un RAT ya que actúa como una medida de control de la información al interior de la organización.

Notificación de incidentes de seguridad

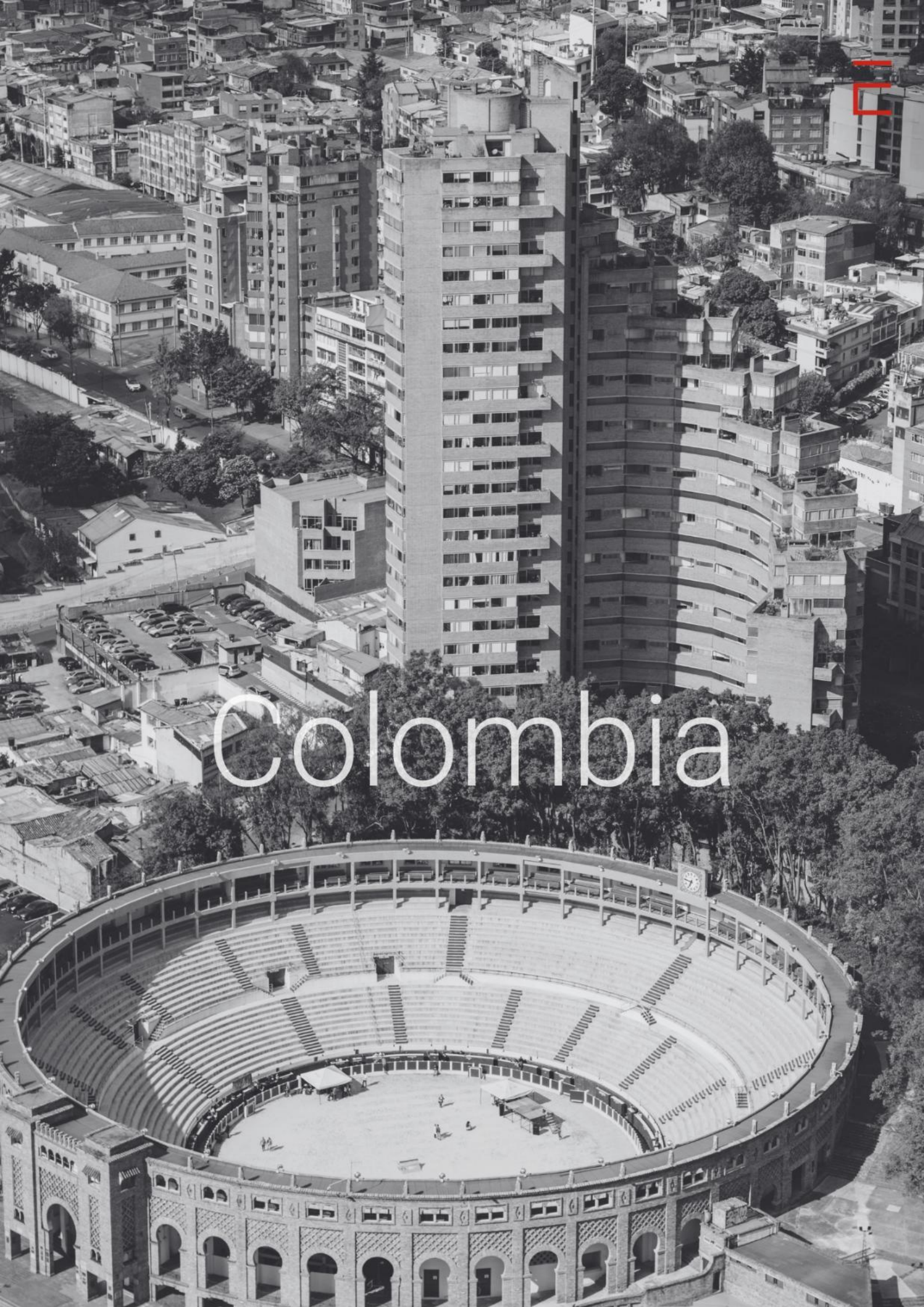
- Se debe reportar a la Agencia de Protección de Datos Personales (“APDP”) por los medios más expeditos posibles y sin dilaciones. Se informará también a los titulares cuando se vean involucrados datos de niños, niñas o adolescentes, datos sensibles o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

Evaluaciones de impacto en el tratamiento de datos personales

- Se exige una EIPD en caso de que el tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, produzca un alto riesgo para los derechos de las personas. Se publicará, por parte de la APDP, un listado de actividades de tratamiento que requerirán una EIPD y los correspondientes lineamientos mínimos para realizarla.

Multas por incumplimiento:

En Chile las multas por incumplimiento son de hasta 20.000 unidades tributarias mensuales (~USD 1.5 millones). En caso de reiteración, esta multa puede alcanzar hasta el 4% de los ingresos anuales o verse triplicada, lo que resulte más gravoso.



Colombia

Colombia en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley N° 1581 de 2012 regula el tratamiento de los datos personales de las personas recogidos en bases de datos o archivos (públicos y privados), así como los derechos, libertades y garantías constitucionales que se refieren en el artículo 15 y 20 de la Constitución Política de Colombia.

¿Cuáles son los derechos de los titulares?

- Los titulares tienen derecho a conocer y rectificar los datos, para acceder a la información, solicitar prueba de la autorización otorgada, presentar quejas Superintendencia de Industria y Comercio ("SIC") y a revocar la autorización y/o solicitar la supresión del dato.

¿Qué deberes tiene la empresa?

- El responsable deberá garantizar a los titulares el ejercicio de sus derechos y también informarles íntegramente respecto de sus solicitudes, conservar sus datos de manera segura y suministrar correctamente su información a los encargados. Asimismo, deberá adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley e informar a la autoridad cuando se presenten violaciones a los códigos de seguridad.

¿Cómo se deben tratar los datos sensibles?

- El tratamiento de datos personales sensibles requiere una autorización calificada del titular la cual deberá ser informada de manera expresa sobre las finalidades específicas del tratamiento y sobre cuáles de sus datos son sensibles. En ningún caso podrá condicionarse la prestación de un servicio al suministro de datos sensibles, como los biométricos.

Encargados de tratamiento de datos personales

- Además de los deberes previstos en la ley, el encargado deberá cumplir las instrucciones del responsable conforme al contrato de transmisión de datos, aplicar las obligaciones derivadas de la política de tratamiento del responsable y garantizar que el encargo se realice únicamente para las finalidades autorizadas por los titulares y en cumplimiento de la normativa aplicable.

¿Se debe contar con un registro de actividades de tratamiento?

- No se establece ninguna regulación respecto el RAT. Sin embargo, la regulación sí exige el registro de las bases de datos en el Registro Nacional de Bases de Datos administrado por la SIC.

Notificación de incidentes de seguridad

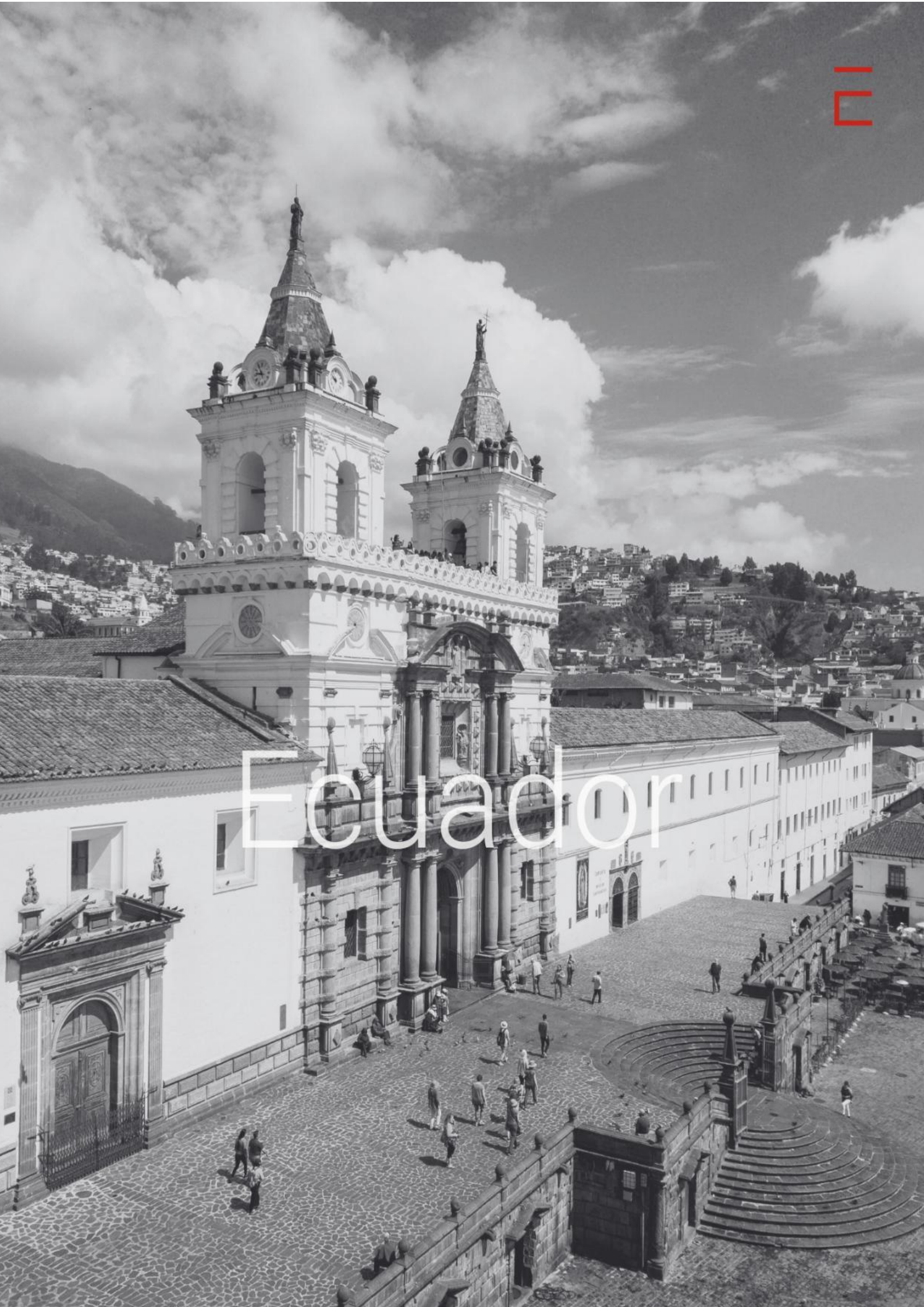
- Se debe reportar a la SIC a más tardar dentro de los 15 días hábiles siguientes al momento en el que se detecten los incidentes. Ahora bien, no es obligatorio, pero sí se considera como una buena práctica el hecho de comunicar a los titulares la información relativa a la brecha ocurrida.

Evaluaciones de impacto en el tratamiento de datos personales

- No se encuentran reglamentadas de manera expresa las EIPD. Sin embargo, la SIC las reconoce como una medida adecuada para demostrar el cumplimiento del principio de responsabilidad demostrada (responsabilidad proactiva).

Multas por incumplimiento:

En Colombia las multas por incumplimiento son por hasta 2.000 salarios mínimos mensuales legales vigentes al momento de la imposición de la norma. Lo anterior puede incluir también la suspensión, cierre temporal o cierre definitivo de las actividades.


Ecuador

Ecuador en materia de protección de datos personales:

¿Qué regula la normativa?

- Artículo 66, numeral 19 de la Constitución de la República. Ley Orgánica de Protección de Datos Personales ("LOPDP") (Registro Oficial Suplemento Nro. 459, 26 de mayo de 2021. Reglamento a la Ley Orgánica de Protección de Datos (Registro Oficial Suplemento No. 478, 15 de diciembre de 2023). La Superintendencia de Protección de Datos Personales ha regulado la materia a través de resoluciones.

¿Cuáles son los derechos de los titulares?

- Se reconocen varios derechos en la normativa, entre los que se encuentran los llamados ARCO+ que consideran el derecho a la información, acceso, rectificación, actualización, eliminación, oposición, suspensión, portabilidad y a no ser objeto de decisiones total o parcialmente automatizadas. También los titulares tienen derecho a realizar consultas al Registro Nacional de Protección de Datos Personales.

¿Qué deberes tiene la empresa?

- Las empresas deben cumplir con los 12 principios que le resultan aplicables y establecer medidas de técnicas (incluidas las de seguridad), organizativas y legales adecuadas al riesgo identificado. Además, deberán notificar los incidentes que afecten datos personales, gestionar los riesgos y también aplicar medidas de protección de datos desde el diseño y por defecto.

¿Cómo se deben tratar los datos sensibles?

- Podrán tratarse bajo consentimiento explícito y excepcionalmente para cumplir obligaciones laborales o de seguridad social, para proteger intereses vitales si el titular no puede consentir, si los datos han sido hechos públicos por el titular, por orden judicial, con fines de archivo, investigación o estadística de interés público, o cuando se trate de datos de salud conforme a la LOPDP.

Encargados de tratamiento de datos personales

- El tratamiento se puede realizar por un tercero bajo instrucciones del responsable. Se debe celebrar un contrato que establezca el objeto del encargo, su duración, naturaleza, finalidad, el tipo de datos tratados, las categorías de los titulares y los derechos y obligaciones de las partes. Una vez finaliza el encargo, los datos deberán ser destruidos o devueltos al responsable en 5 días.

¿Se debe contar con un registro de actividades de tratamiento?

- El responsable del tratamiento deberá contar con un RAT en la medida que cuente con cien o más trabajadores, o cuando se cumplan las siguientes condiciones: i) el tratamiento entraña un riesgo para los derechos y libertades, ii) no sean tratamientos

ocasionales, iii) incluya categorías especiales de datos. El encargado también deberá llevar el registro cuando el responsable esté obligado a ello.

Notificación de incidentes de seguridad

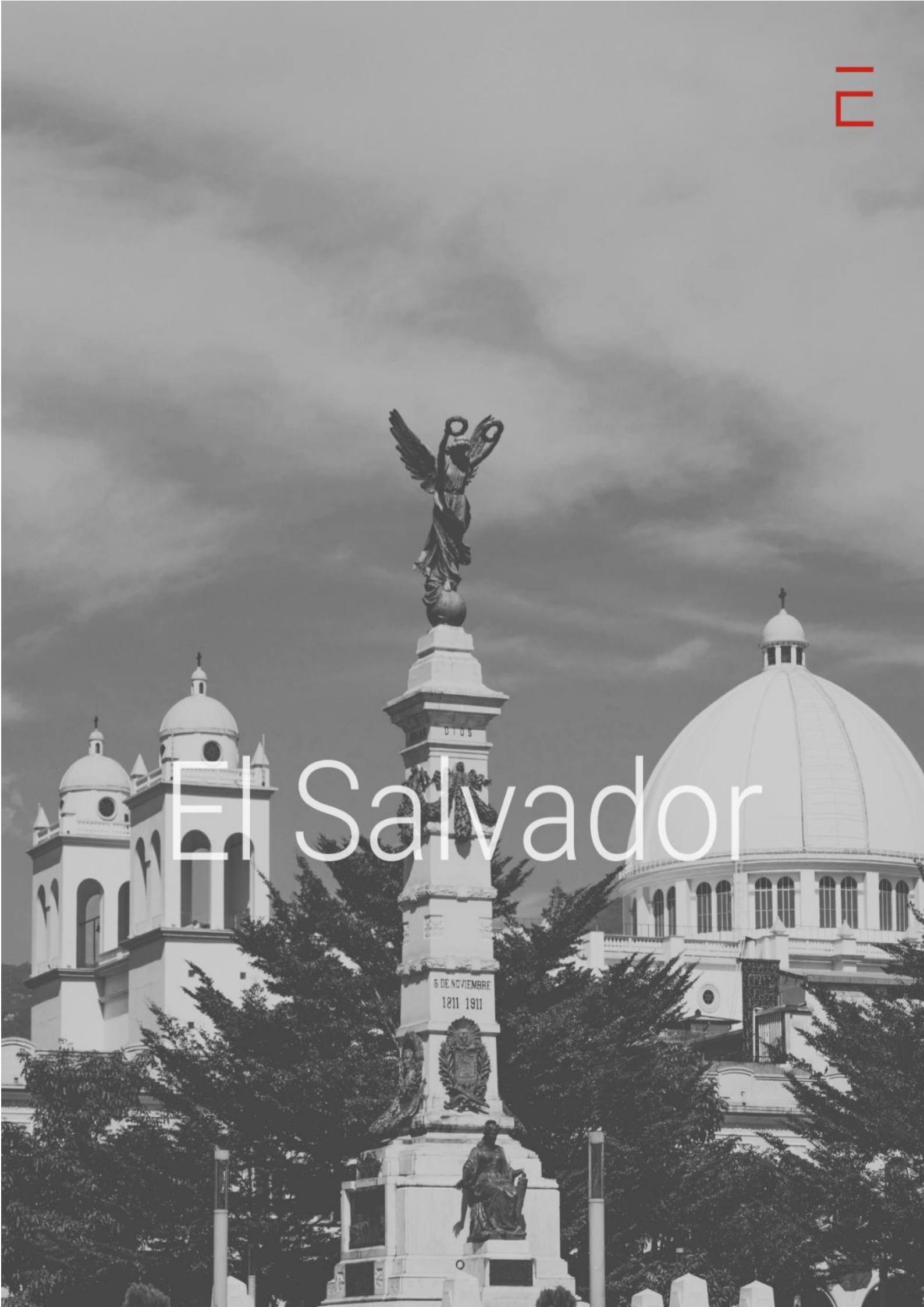
- Se debe reportar a la Superintendencia de Protección de Datos Personales (“SPDP”) y a la Agencia de Regulación y Control de las Telecomunicaciones (“ARCOTEL”) en un plazo máximo de 5 días. Se informará también a los titulares cuando se identifiquen riesgos a sus derechos y libertades en un plazo máximo de 3 días.

Evaluaciones de impacto en el tratamiento de datos personales

- Por regla general se exige una EIPD cuando se detecte la probabilidad de que el tratamiento conlleve riesgos para los derechos de los titulares. En esa línea, será obligatoria cuando exista una elaboración automatizada de perfiles, sea un tratamiento a gran escala de categorías especiales, haya una observación sistemática a gran escala en zonas de acceso público, o se utilicen datos biométricos.

Multas por incumplimiento:

En Ecuador las multas por incumplimiento son de hasta el 1% del volumen de los negocios correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.



El Salvador

El Salvador en materia de protección de datos personales:

¿Qué regula la normativa?

- El Decreto N° 144 contiene la Ley para la Protección de Datos Personales, la cual tiene por objeto establecer la regulación de estos, la determinación de los requisitos esenciales para el tratamiento legítimo y el marco normativo que debe seguirse.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos ARCO-POL: Acceso, Rectificación, Cancelación, Oposición, Portabilidad y Limitación. La presentación de la solicitud deberá realizarse el Delegado de Protección de Datos, quien tendrá un plazo de 20 días hábiles para responder a la solicitud, con posibilidad de prorrogarlo por 20 días hábiles más.

¿Qué deberes tiene la empresa?

- El tratamiento de datos personales deberá ajustarse a los principios y obligaciones establecidos en la Ley de Desarrollo y Protección Social, incluyendo la implementación y mantenimiento permanente de medidas técnicas, organizativas y de seguridad adecuadas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales, así como para prevenir accesos no autorizados, pérdida, alteración o divulgación indebida durante todo su ciclo de vida.

¿Cómo se deben tratar los datos sensibles?

- Sólo podrán tratarse con el consentimiento expreso e inequívoco del titular. Excepcionalmente podrán tratarse también cuando sea para la salvaguarda de la vida del titular, para la prevención o diagnóstico médico, cuando medien razones de interés general autorizadas por alguna otra ley o cuando el responsable tenga mandato legal para ello.

Encargados de tratamiento de datos personales

- El encargado, o el Delegado de Protección de Datos, además de cumplir con los principios establecidos en la ley, deberá limitar el tratamiento a la finalidad para cual se emitió el consentimiento, implementar medidas de seguridad acordes, guardar confidencialidad y con toda otra obligación que le atribuya la normativa.

¿Se debe contar con un registro de actividades de tratamiento?

- La normativa salvadoreña no exige expresamente la implementación de un RAT. Sin embargo, se recomienda contar con uno desde el inicio, ya que permite monitorear y supervisar el tratamiento de datos personales dentro de la organización, sirve como medida interna de control y facilita la adaptación ante eventuales exigencias regulatorias futuras.

Notificación de incidentes de seguridad

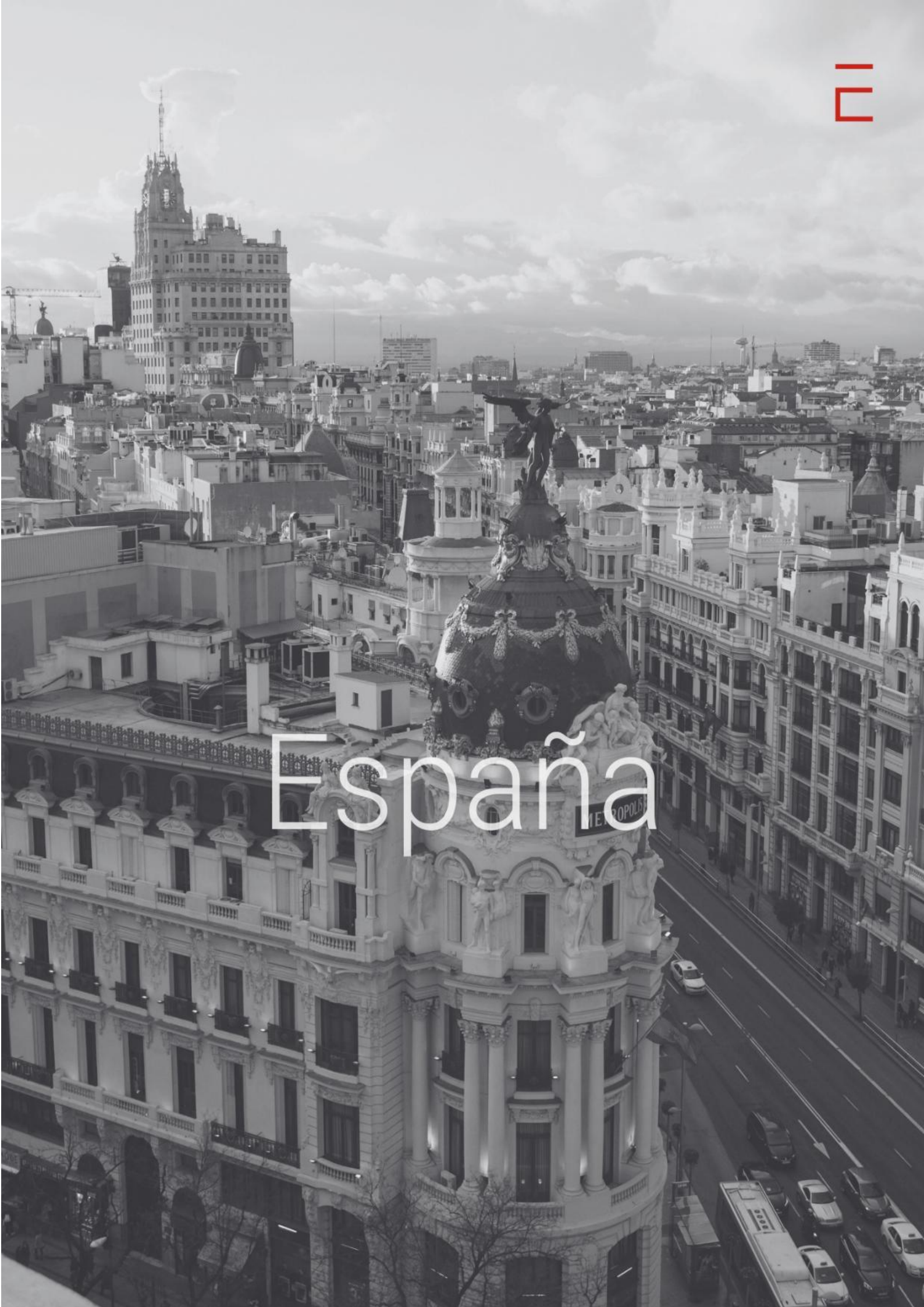
- Ante una vulneración de seguridad, el responsable deberá notificar a la Agencia de Ciberseguridad del Estado, a la Fiscalía General de la República y los titulares afectados dentro de un plazo máximo de 72 horas desde que tomó conocimiento del suceso. Además, el responsable deberá iniciar un proceso de revisión exhaustiva respecto el incidente.

Evaluaciones de impacto en el tratamiento de datos personales

- La ley vigente no regula este asunto. Sin embargo, se recomienda realizar evaluaciones de impacto, de acuerdo con los estándares internacionales, en vistas a cumplir con la responsabilidad proactiva.

Multas por incumplimiento:

En El Salvador las multas por incumplimiento alcanzan hasta máximo de 40 salarios mínimos mensuales vigentes del sector de comercio.


España

España en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley Orgánica 3/2018 tiene por objeto adaptar la aplicación del Reglamento General de Protección de Datos ("RGPD") en el ordenamiento jurídico español y garantizar los derechos digitales de la ciudadanía conforme a lo establecido en el artículo 18.4 de la Constitución Española relacionado con el respeto al honor y la intimidad en el uso de la informática.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos determinados en el RGPD en los artículos 15 a 22, es decir, el de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición al tratamiento y también a no ser objeto de decisiones individuales automatizadas. El responsable tiene un mes para responder a la solicitud, con posibilidad de ampliarse el plazo.

¿Qué deberes tiene la empresa?

- Se deberán cumplir con los principios y obligaciones determinadas en el RGPD como son los de analizar los riesgos de sus actividades e implementar medidas adecuadas considerando dicho riesgo. Por otra parte, debe valorar la existencia de tratamientos de alto riesgo y, en determinados casos, designar un Delegado de Protección de Datos.

¿Cómo se deben tratar los datos sensibles?

- Con carácter general, está prohibido el tratamiento de categorías especiales de datos relacionados con el sexo, la raza, afiliación sindical o política, creencia religiosa, entre otros. Existen excepciones para su tratamiento relacionadas con la existencia de obligaciones en materia laboral, intereses públicos esenciales o, entre otras, el consentimiento explícito del interesado.

Encargados de tratamiento de datos personales

- Se regula la relación del responsable con el encargado por un contrato que vincule a ambas partes. Se establecerá el objeto, duración, naturaleza y finalidad del tratamiento, el tipo de datos y categoría de los interesados, y las obligaciones y derechos de las partes. El encargado debe otorgar garantías suficientes considerando el tratamiento.

¿Se debe contar con un registro de actividades de tratamiento?

- Será obligatorio llevar un RAT para todas aquellas empresas que empleen a más de 250 personas, a menos que el tratamiento que los responsables realicen entrañe un riesgo para los derechos y libertades de los titulares, no sea ocasional o incluya datos de categoría especial o de condenas e infracciones penales. Las administraciones públicas deberán mantener publicado su registro de actividades de tratamiento.

Notificación de incidentes de seguridad

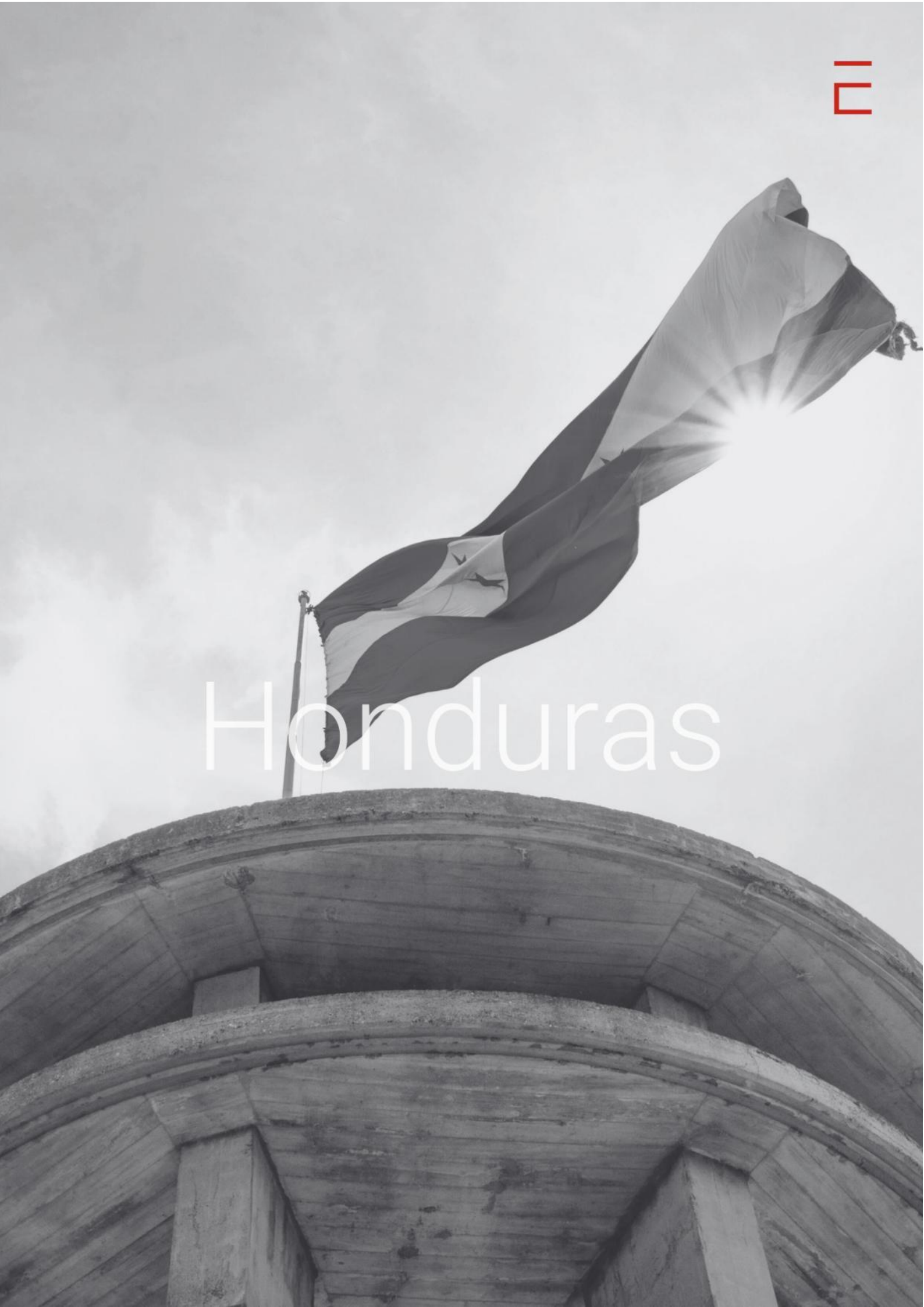
- Se debe notificar a la Agencia Española de Protección de Datos ("AEPD") toda brecha que pueda suponer un riesgo para los derechos y libertades de los titulares, sin dilación indebida y dentro de un plazo de 72 horas contadas a partir de que se conozca el incidente. Será notificada a los interesados únicamente si esta brecha entraña un alto riesgo para ellos.

Evaluaciones de impacto en el tratamiento de datos personales

- Se realizará una EIPD ante aquellas situaciones en donde, por la naturaleza, alcance, contexto o fines de la actividad, especialmente si se utilizan nuevas tecnologías, exista alto riesgo para los derechos de los interesados. La AEPD, por su parte, podrá exonerar determinados tratamientos de la realización de una EIPD y obligar a la realización de otros.

Multas por incumplimiento:

En España las multas por incumplimiento son de hasta 20 millones de euros (~USD 23 millones aproximadamente) o el 4% del volumen de negocios anual a nivel mundial, lo que sea mayor.


Honduras

Honduras en materia de Protección de Datos Personales:

¿Qué regula la normativa?

- Actualmente está en discusión legislativa una ley específica que regula el tratamiento de datos. Sin embargo, algunos aspectos sobre datos personales se regulan en la legislación vigente, como la Ley de Transparencia y Acceso a la Información Pública o la Ley del Registro Nacional de las Personas. Además, en el artículo 76 de la Constitución Política se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

¿Cuáles son los derechos de los titulares?

- Mediante la garantía constitucional del "Habeas Data", los titulares tienen el derecho a acceder a la información sobre estos o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.

¿Qué deberes tiene la empresa?

- Las empresas, en vistas al manejo de bases de datos e información personal de los titulares, deberán ceñirse a las buenas prácticas y lineamientos que cada cual determine, protegiendo el honor, intimidad personal y la propia imagen por disposición constitucional y normativa penal que prevé penas de prisión a quienes divulguen, revelen o cedan cualquier documento, papel, datos, información en cualquier soporte o efectos personales, según el artículo 272 del Código Penal.

¿Cómo se deben tratar los datos sensibles?

- No existe una regulación respecto a las bases habilitantes para el tratamiento de los datos personales sensibles. Sin embargo, se recomienda adecuarse a estándares internacionales como el Reglamento General de Protección de Datos respecto las bases que permiten el tratamiento de esta información.

Encargados de tratamiento de datos personales

- No hay regulación específica respecto el tratamiento de datos por medio de encargados de tratamiento.

¿Se debe contar con un registro de actividades de tratamiento?

- No se estipula nada respecto el RAT. Sin embargo, se recomienda contar con uno, ya que esto permitirá identificar, conocer y supervisar las actividades de tratamiento de datos en las entidades. Además, permite individualizar los datos personales utilizados y los encargados que participan del tratamiento de datos.

Notificación de incidentes de seguridad

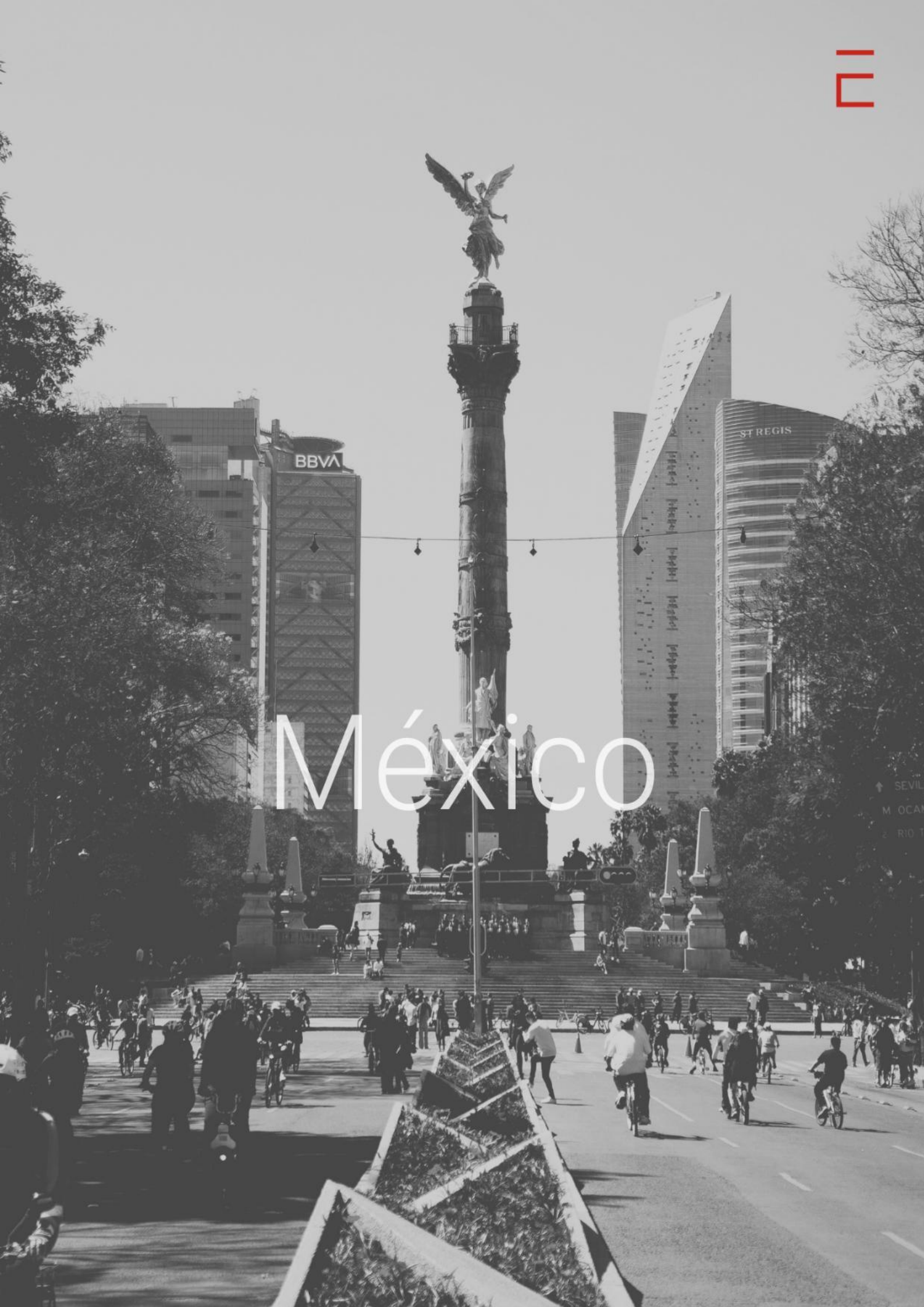
- No existe ninguna entidad a la cual reportar en caso de que se produzca una brecha de seguridad. El manejo de las crisis depende únicamente del responsable del tratamiento.

Evaluaciones de impacto en el tratamiento de datos personales

- No existe una regulación respecto las EIPD. Sin embargo, se recomienda adecuarse a estándares internacionales como el RGPD respecto de todos aquellos tratamientos que involucren una evaluación.

Multas por incumplimiento:

En Honduras, actualmente, no existen sanciones ni multas aparejadas al incumplimiento de las obligaciones por parte del responsable de datos.



México

Mexico en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPDPPP"), reformada en 2025, tiene por objeto proteger los datos personales en posesión de particulares, regulando su tratamiento legítimo, controlado e informado para garantizar la privacidad y la autodeterminación informativa previstas en el artículo 16 constitucional. Establece principios, deberes, derechos, obligaciones, esquemas de autorregulación y sanciones.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos ARCO: Acceso, Rectificación, Cancelación y Oposición. El responsable debe habilitar medios gratuitos, accesibles y claros para el ejercicio de los derechos, atender las solicitudes sin obstáculos y dentro de los plazos legales. Estas condiciones, deben establecerse con precisión en el aviso de privacidad.

¿Qué deberes tiene la empresa?

- El responsable debe cumplir con los principios previstos en la LFPDPPP —licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad— así como garantizar el cumplimiento de los deberes de seguridad y confidencialidad mediante la implementación de medidas administrativas, técnicas y físicas adecuadas al riesgo del tratamiento.

¿Cómo se deben tratar los datos sensibles?

- Su tratamiento exige consentimiento expreso y por escrito, salvo las excepciones legales: disposición jurídica, fuentes públicas, datos disociados, ejercicio de derechos u obligaciones contractuales, emergencias, atención médica bajo secreto profesional u orden de autoridad. Su uso debe ser limitado, justificado y con seguridad reforzada.

Encargados de tratamiento de datos personales

- La relación responsable–encargado debe formalizarse mediante un contrato u otro instrumento jurídico que acredite su existencia y defina el alcance, las finalidades, el tipo de datos, las medidas de seguridad aplicables, la prohibición de usarlos para fines distintos y la supresión o devolución de la información al concluirlo. Todo tratamiento deberá ser congruente con el aviso de privacidad.

¿Se debe contar con un registro de actividades de tratamiento?

- Si bien no es obligatorio por mandato expreso, su elaboración constituye un elemento estructural del cumplimiento, al permitir la trazabilidad e identificación de los tratamientos, su ciclo de vida y los riesgos asociados. Esto facilita la gestión de riesgos, refuerza el principio de responsabilidad y se convierte en una práctica necesaria para acreditar el deber de seguridad previsto en la normativa mexicana.

Notificación de incidentes de seguridad

- El responsable deberá activar de inmediato un procedimiento de análisis y contención ante cualquier vulneración y, una vez confirmada y evaluada su afectación, deberá notificar sin dilación al titular cuando ésta pueda impactar de forma significativa sus derechos patrimoniales o morales, para que adopte medidas de protección.

Evaluaciones de impacto en el tratamiento de datos personales

- La EIPD no es obligatoria; estas evaluaciones son atribución de la Secretaría Anticorrupción y Buen Gobierno dentro de su ámbito de competencia. En el sector privado, su elaboración voluntaria es una buena práctica que se alinea con los estándares internacionales, y que es recomendable antes de nuevos tratamientos o modificaciones sustanciales para anticipar riesgos y para reforzar el cumplimiento del principio de responsabilidad, proporcionalidad y deber de seguridad.

Multas por incumplimiento:

En México las multas por incumplimiento son de hasta 320.000 Unidades de Medida y Actualización (~USD 1.9 millones aproximadamente) y con posibilidad de incrementarse hasta dos veces si se relacionan con datos personales sensibles y de aplicar multas adicionales en caso de reincidencia.


Nicaragua

Nicaragua en materia de Protección de Datos Personales:

¿Qué regula la normativa?

- La Ley N° 787, Ley de Protección de Datos Personales, publicada el 29 de marzo de 2012, tiene por objeto proteger a las personas naturales y jurídicas frente al tratamiento de sus datos personales contenidos en ficheros, tanto públicos como privados. Su finalidad es salvaguardar el derecho a la privacidad personal y familiar, protegido por el artículo 27, numeral 5, de la Constitución Política de la República de Nicaragua.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos de oposición, acceso, modificación, supresión, bloqueo, inclusión, complementación, rectificación y cancelación. Estos deberán ejercerse por escrito y responderse dentro de 10 días hábiles. Ante una ausencia de respuesta, el titular puede ejercer una acción de protección de datos personales. Se reconoce también el derecho al olvido digital en redes sociales, navegadores y servidores.

¿Qué deberes tiene la empresa?

- El responsable deberá utilizar los datos personales exclusivamente para los fines para los cuales fueron recabados. Deberá adoptar medidas técnicas y organizativas que garanticen la seguridad de los datos, evitado su pérdida, divulgación o acceso no autorizado. Asimismo, deberá asegurar el ejercicio de los derechos del titular, incluidos el acceso, rectificación y cancelación de la información.

¿Cómo se deben tratar los datos sensibles?

- Podrán ser tratados por razones de interés general con el consentimiento del titular o por mandato judicial. También, podrán tratarse de forma estadística o científica de forma anonimizada. Los antecedentes penales o faltas administrativas podrán tratarse por las autoridades competentes según sus atribuciones. Se prohíbe la creación de ficheros de datos sensibles, salvo lo dispuesto por la ley.

Encargados de tratamiento de datos personales

- Se permite que un responsable realice su tratamiento por medio de un encargado, relación la cual se regulará por un contrato celebrado entre las partes. Además, el encargado deberá adoptar medidas de índoles técnicas y organizativas necesarias para la seguridad de los datos personales.

¿Se debe contar con un registro de actividades de tratamiento?

- No es obligatorio contar con un RAT. Sin embargo, se derivan obligaciones que hacen recomendable mantener uno, ya que se deben adoptar medidas técnicas y organizativas para garantizar la seguridad, integridad y confidencialidad de los datos, así como la promoción, de parte de la Dirección de Protección de Datos Personales (“DIPRODAP”),

de modelos de autorregulación para garantizar el derecho a la autodeterminación informativa.

Notificación de incidentes de seguridad

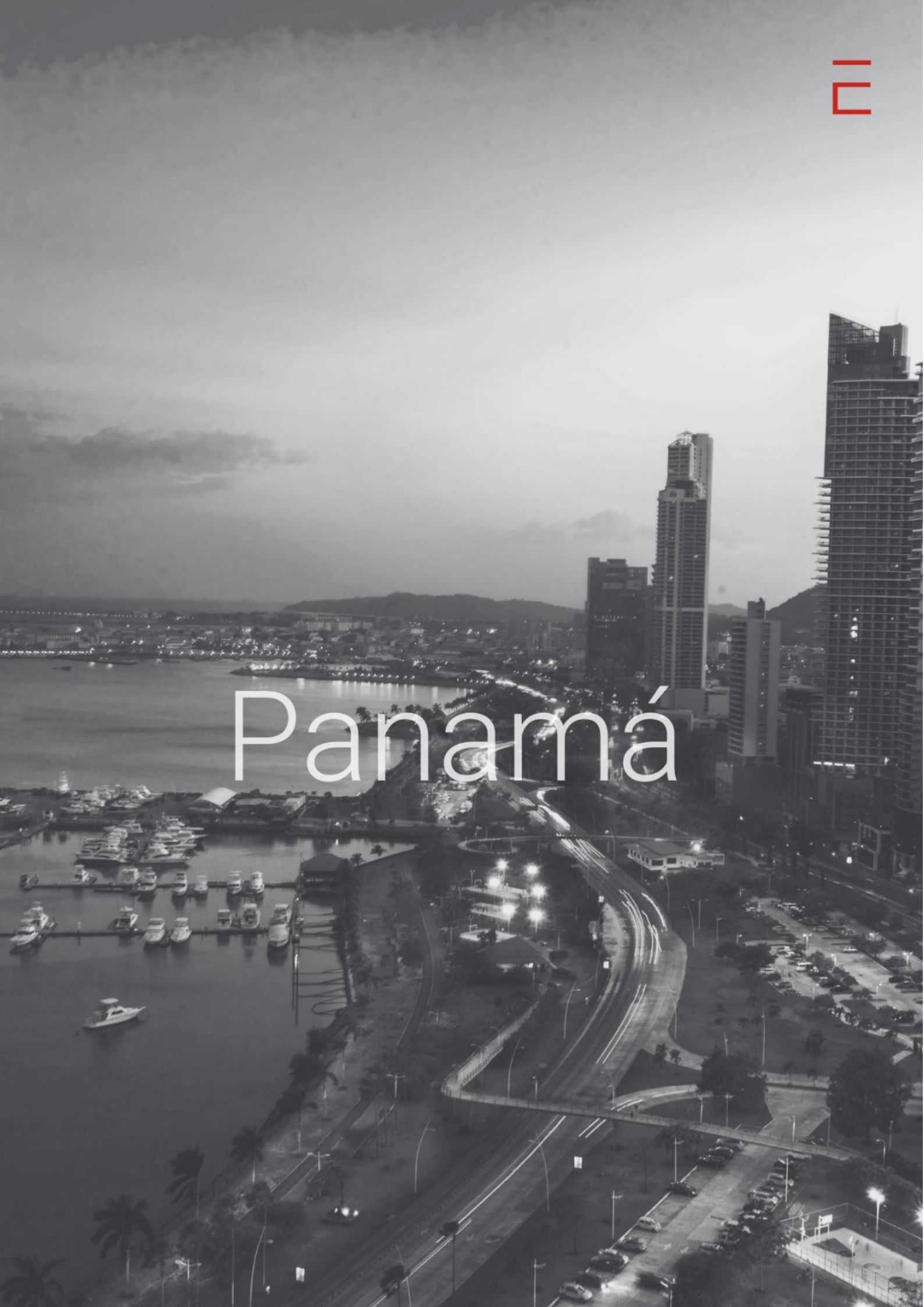
- El incidente deberá reportarse a la DIPRODAP, autoridad competente en materia de protección de datos personales, con facultades de emisión y supervisión de las normas; no obstante, pese a contar con ley y reglamento vigentes, a la fecha no se encuentra operativa en la práctica.

Evaluaciones de impacto en el tratamiento de datos personales

- A pesar de que la EIPD no es obligatoria, en el sector privado, su elaboración voluntaria es una buena práctica alineada con estándares internacionales, recomendable antes de nuevos tratamientos o modificaciones sustanciales para anticipar riesgos y reforzar el cumplimiento del principio de responsabilidad, proporcionalidad y deber de seguridad.

Multas por incumplimiento:

En Nicaragua se aplican sanciones administrativas de apercibimiento, suspensión de operaciones relacionadas con el tratamiento de datos y la clausura o cancelación de los ficheros.


Panamá

Panamá en materia de Protección de Datos Personales:

¿Qué regula la normativa?

- La Ley 81 de 2019 y el Decreto Ejecutivo N° 285 de 28 de mayo de 2021, que reglamenta dicha ley, tiene por objeto establecer los principios, derechos y obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de las personas.

¿Cuáles son los derechos de los titulares?

- Se reconocen como derechos irrenunciables básicos los siguientes: Acceso, Rectificación, Cancelación, Oposición y Portabilidad. Estos derechos se ejercen sobre la base de los principios de lealtad, finalidad, proporcionalidad, veracidad y exactitud, seguridad de los datos, transparencia, confidencialidad y licitud.

¿Qué deberes tiene la empresa?

- El responsable se preocupará de tratar los datos personales bajo el respeto de los derechos fundamentales de los titulares y el ejercicio de los mismos, sobre la base que la ley reconoce al titular. Además, velará por la seguridad de ellos y por tratarlos de forma transparente, lícita, confidencial, proporcional, leal y acorde a la finalidad para la cual fueron recogidos.

¿Cómo se deben tratar los datos sensibles?

- A pesar de que la normativa distingue entre los datos personales comunes y sensibles, establece las mismas bases legales para el tratamiento de ambos tipos de datos. Únicamente determina que cuando el consentimiento refiera a datos personales sensibles y de salud, éste deberá ser previo, irrefutable y expreso.

Encargados de tratamiento de datos personales

- Se regula un mandato por parte del responsable al custodio en el que se tendrá que establecer los protocolos, procesos y procedimientos de gestión y transferencia segura de datos, así como las garantía suficientes para aplicar las medidas técnicas y organizativas adecuadas tales como: autorregulación vinculante, oficial de datos, certificaciones y /o auditorias.

¿Se debe contar con un registro de actividades de tratamiento?

- No se establece ninguna regulación respecto el RAT. Siempre y cuando no se transfieran esos datos a terceros donde si se tendrá que contar con un registro de actividades de tratamiento Sin embargo, la regulación sí exige al responsable documentar qué hace con los datos bajo independientemente los transfiera o no sobre la base de un RAT.

Notificación de incidentes de seguridad

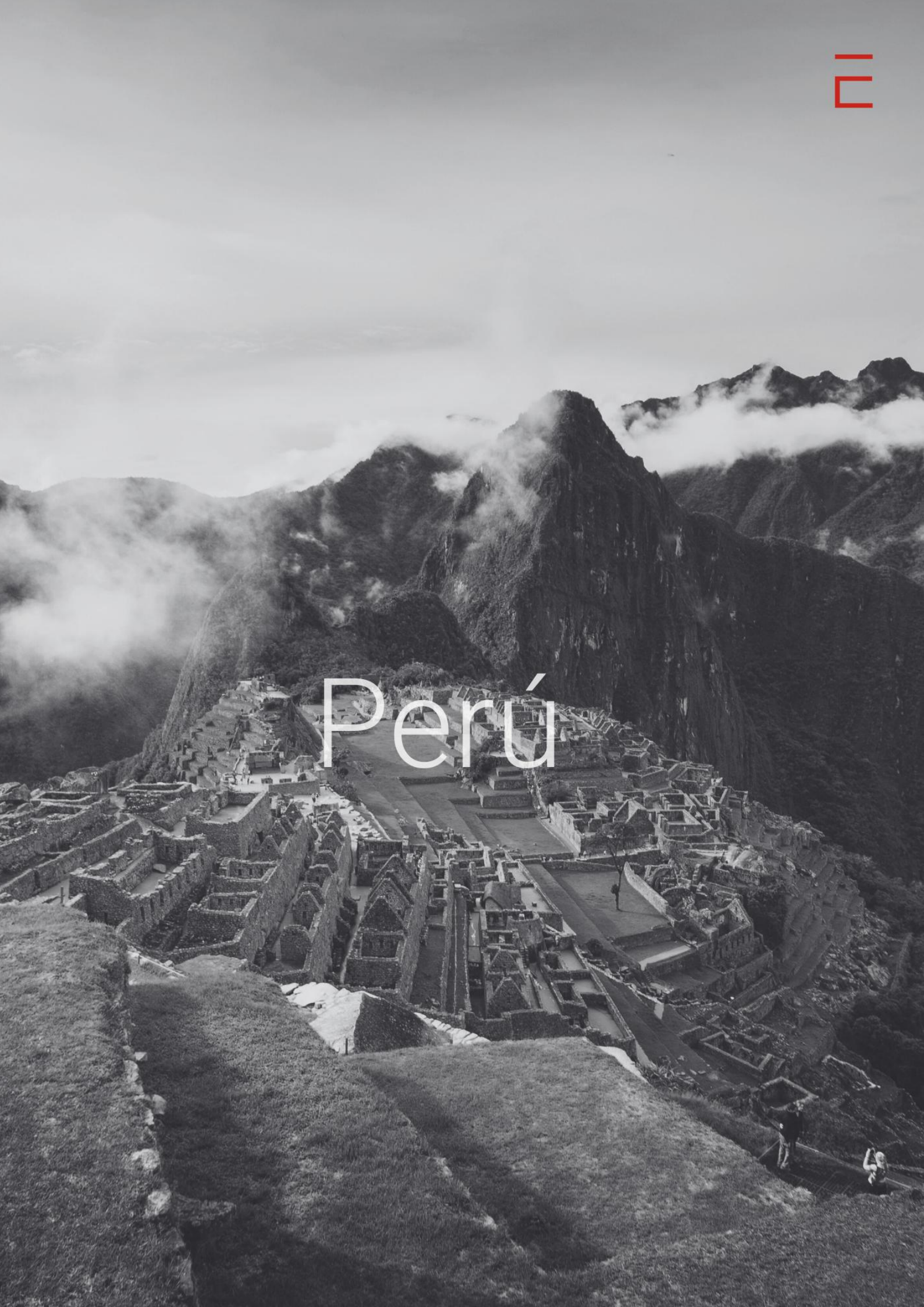
- Se debe notificar a la Autoridad Nacional de Transparencia y Acceso a la Información ("ANTAI") y a los titulares de datos involucrados en un periodo de 72 horas contados a partir de que se conozca el incidente.

Evaluaciones de impacto en el tratamiento de datos personales

- No hay una regulación expresa. En razón de ello, queda a criterio de la autoridad de control, en este caso, la ANTAI, definir los supuestos en los que se requerirán evaluaciones de impacto, bajo el principio de la proporcionalidad.

Multas por incumplimiento:

En Panamá las multas por incumplimiento son de hasta 10.000 balboas panameñas (~USD 10.000). Las sanciones pueden incluir la clausura de la base de datos y la suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de forma temporal o permanente.


Perú

Perú en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley N° 29.733, promulgada el 21 de junio de 2011, tiene por objeto garantizar el derecho fundamental previsto en el artículo 2 numeral 6 de la Constitución Política de Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en esta se reconocen. Además, se desarrolla mediante el Reglamento de Protección de Datos Personales, cuya última versión fue aprobada por Decreto Supremo N° 16-2024-JUS.

¿Cuáles son los derechos de los titulares?

- Se reconoce a los titulares los derechos de información, acceso, portabilidad, actualización, rectificación, inclusión, cancelación, oposición y al tratamiento objetivo de datos personales. El responsable deberá dar respuesta en tiempo y plazo de acuerdo a la ley y debe facilitar un procedimiento sencillo para el ejercicio de estos derechos.

¿Qué deberes tiene la empresa?

- El responsable del tratamiento de datos personales debe cumplir con los principios y obligaciones determinados en la normativa. Del mismo modo, deberá implementar un documento de seguridad y designar a un Oficial de Datos Personales (ODP) según sea el caso, entre otras obligaciones establecidas en la normativa.

¿Cómo se deben tratar los datos sensibles?

- Sólo pueden tratarse con el consentimiento por escrito del titular, mediante firma manuscrita, digital, electrónica o cualquier otra modalidad que garantice de forma inequívoca manifestación de su voluntad. En su excepción, podrán tratarse siempre que la ley lo autorice y que ello atienda a motivos de importante interés público.

Encargados de tratamiento de datos personales

- El encargado debe tratar los datos personales solo para los fines y plazos pactados con el titular, no podrá transferirlos sin autorización y deberá cumplir con los deberes de confidencialidad y seguridad. Al concluir el servicio, los datos se suprimirán en un plazo máximo de dos (2) años del último encargo. El subencargo requiere autorización del responsable.

¿Se debe contar con un registro de actividades de tratamiento?

- No es obligatorio mantener un RAT conforme a la normativa peruana. No obstante, es recomendable mantener un documento que recoja este detalle, que permita la identificación de los tratamientos de datos personales y contribuir a una gestión de los datos con un enfoque de riesgo.

Notificación de incidentes de seguridad

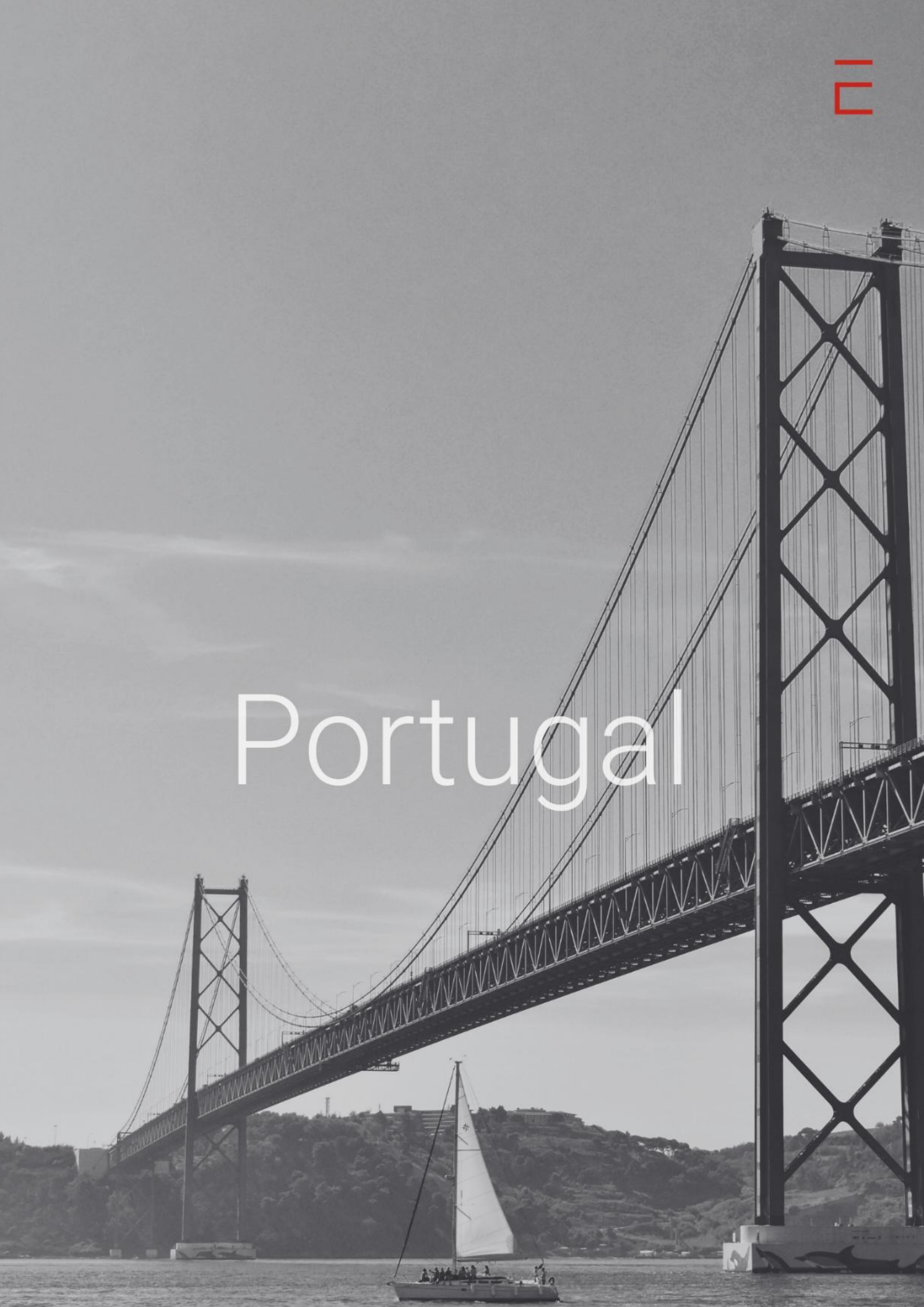
- Ante incidentes que afecten gravemente al titular o involucren grandes volúmenes de datos, entre otros supuestos, se debe notificar a la Autoridad Nacional de Protección de Datos Personales en un plazo de 48 horas, detallando el suceso y las medidas de mitigación, de acuerdo a los lineamientos publicados. También se informará al titular de forma clara, brindando recomendaciones y nuevos hallazgos.

Evaluaciones de impacto en el tratamiento de datos personales

- De manera facultativa y previa, el responsable puede realizar la EIPD, en especial cuando se trate de datos sensibles, exista una elaboración de perfiles o sea un tratamiento masivo de datos, entre otros supuestos. Para su realización, se deberán observar las Directivas y los lineamientos establecidos por la Autoridad Nacional de Protección de Datos Personales.

Multas por incumplimiento:

En Perú las multas por incumplimiento son de hasta 100 Unidades Impositivas Tributarias en caso de persistir el incumplimiento (~USD 164.000 aproximadamente) o hasta el límite 10% de ingresos netos del año anterior.


Portugal

Portugal en materia de Protección de Datos Personales:

¿Qué regula la normativa?

- La Ley N° 58/2019 de 8 de agosto, tiene por objeto regular la aplicación del Reglamento General de Protección de Datos en el ordenamiento jurídico portugués.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos previstos en el RGPD, en particular los de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, así como el derecho a no ser objeto de decisiones basadas exclusivamente en tratamientos automatizados, incluida la elaboración de perfiles. El responsable debe habilitar canales para su ejercicio y responder en el plazo de un mes, prorrogable.

¿Qué deberes tiene la empresa?

- Se obliga a tener un Delegado de Protección de Datos Personales en todas aquellas entidades públicas o privadas que realicen un tratamiento de datos sensibles o lo hagan a gran escala. Además, tienen deber de confidencialidad para todos los colaboradores con acceso a datos, de aplicar las medidas técnicas y organizativas apropiadas y de respetar los principios determinados en el RGPD.

¿Cómo se deben tratar los datos sensibles?

- Podrán tratarse con el consentimiento explícito del titular o, en determinados casos, por obligación legal o por motivos de seguridad, para proteger intereses vitales, en el marco de actividades legítimas de entidades sin ánimo de lucro, cuando el interesado los haya hecho manifiestamente públicos, por razones de interés público o de salud, o para la formulación o la defensa de reclamaciones.

Encargados de tratamiento de datos personales

- El responsable y encargado deben formalizar su relación por medio de un contrato vinculante que fije objeto, duración, naturaleza y finalidad, tipos de datos y categorías de interesados. El responsable recurre solo a encargados con garantías de medidas técnicas y organizativas adecuadas, y el encargado trata los datos únicamente según instrucciones documentadas.

¿Se debe contar con un registro de actividades de tratamiento?

- Será obligatorio llevar un RAT para todas aquellas empresas que empleen a más de 250 personas, a menos que los tratamientos que realicen los responsables entrañe un riesgo para los derechos y libertades de los titulares, no sea ocasional o incluya datos sensibles o relativos a condenas e infracciones penales.

Notificación de incidentes de seguridad

- Ante una violación de seguridad que ponga en riesgo los derechos y libertades de los titulares, se debe notificar a la Comisión Nacional de Protección de Datos ("CNPD") sin dilación indebida y, en su caso, dentro de 72 horas desde que se tenga conocimiento, sin perjuicio de su registro interno. El interesado solo será informado cuando la violación entrañe un alto riesgo para sus derechos y libertades.

Evaluaciones de impacto en el tratamiento de datos personales

- Deberá realizarse una EIPD ante aquellas situaciones en que por la naturaleza, alcance, contexto o fines de la actividad, se entrañe un alto riesgo para los derechos de los interesados. La CNPD, sin embargo, podrá exonerar, mediante una lista, determinados tratamientos de la realización de una EIPD. En este contexto, el Reglamento Nº 798/2018 de la CNPD determina las actividades de tratamiento de datos personales sujetas a la realización de una EIPD.

Multas por incumplimiento:

En Portugal las multas por incumplimiento son de hasta 10 millones de euros (~USD 11.5 millones aproximadamente) o el 2% del volumen de negocios anual mundial, lo que sea mayor, para infracciones graves. Respecto las muy graves, las multas pueden ser de hasta 20 millones de euros o el 4%.


Puerto Rico

Puerto Rico en materia de protección de datos personales:

¿Qué regula la normativa?

- Se regula por medio de la Ley Num. 111-2005 ("*Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información*"), la Ley Num. 39-2012 ("*Ley de Notificación de Política de Privacidad*"), la Ley Num. 185 de 2024 ("*Ley para la Protección de la Privacidad Cibernética de los Niños y Jóvenes*") y el Reglamento Num. 8.568 del 27 de febrero de 2015 que regula publicación de políticas de privacidad en el manejo de datos personales. Además de vasta legislación federal estadounidense.

¿Cuáles son los derechos de los titulares?

- No existe una ley que reconozca expresamente un catálogo uniforme de derechos de titulares, sino que nos debemos regir por el derecho constitucional a la intimidad, legislación sectorial previamente mencionada y las leyes federales aplicables a las diferentes industrias.

¿Qué deberes tiene la empresa?

- Se deberán cumplir con los principios y obligaciones determinadas en las normativas, deberán implementar medidas de seguridad razonables, notificar cualquier tipo de incidente o transgresión de seguridad y evitar toda divulgación no autorizada de datos personales. Es importante tomar en consideración la industria de la empresa para el cumplimiento adecuado de la normativa correspondiente.

¿Cómo se deben tratar los datos sensibles?

- Respecto las normativas vigentes, únicamente se hace mención, respecto la privacidad cibernética, de que toda información personal de usuarios menores de edad no podrá ser publicadas o divulgadas con el consentimiento expreso de estos y la padre, madre o tutor.

Encargados de tratamiento de datos personales

- Las normativas vigentes no regulan la relación entre el responsable y el encargado. Sin embargo, se recomienda contar con contrato que establezca los derechos y obligaciones de las partes, el resguardo de la información personal, la duración del encargo y la finalidad del tratamiento.

¿Se debe contar con un registro de actividades de tratamiento?

- En las normativas no se hace mención alguna sobre el RAT. Sin embargo, se recomienda que los responsables de datos identifiquen todas aquellas actividades que involucren el tratamiento de información personal en vistas a contar con medidas internas de control.

Notificación de incidentes de seguridad

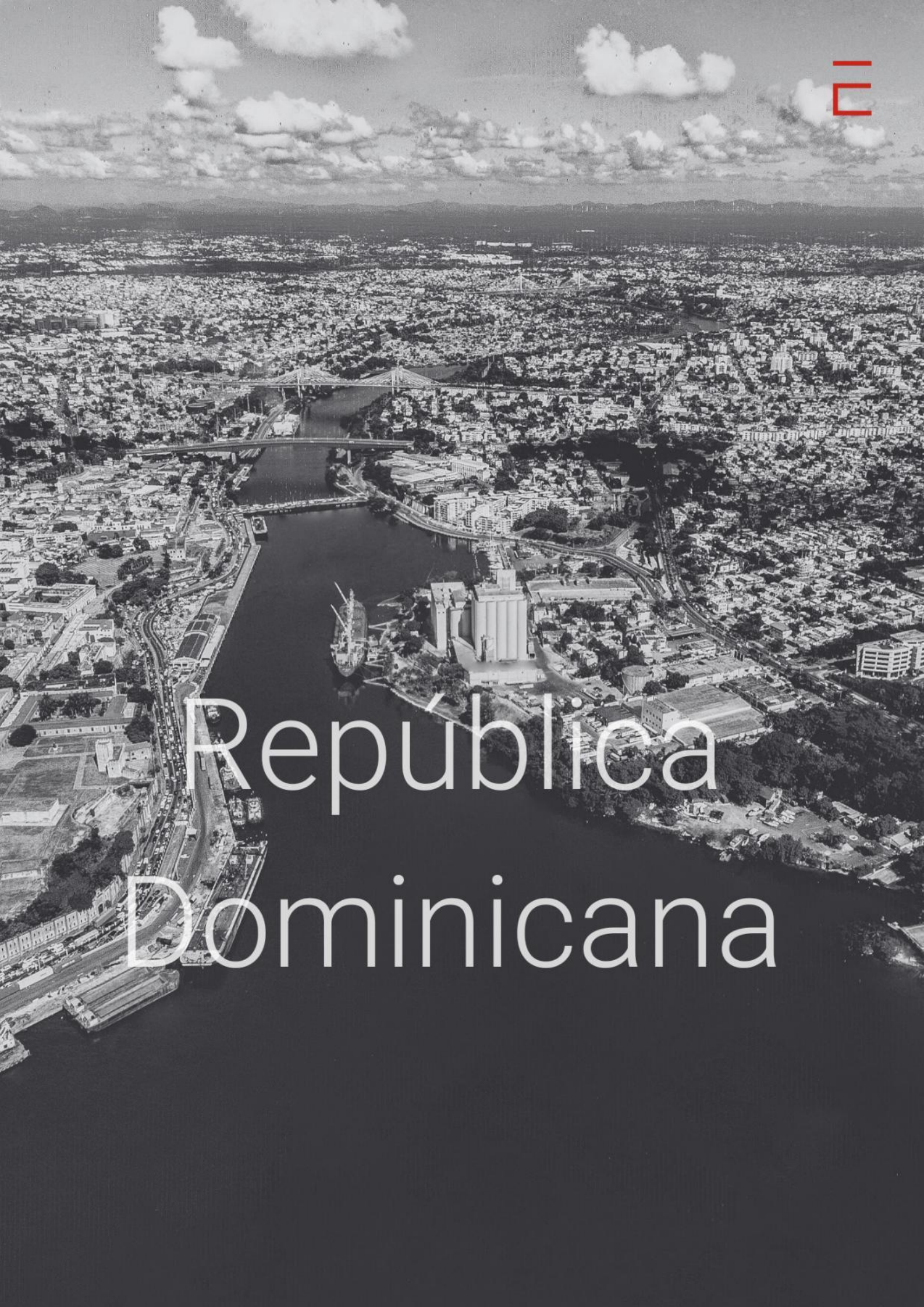
- Dentro de un plazo improrrogable de 10 días, el responsable deberá información de la vulneración de seguridad al Departamento de Asuntos del Consumidor. Además, deberá informarse, por el medio más expedito posible, a los titulares afectados de la brecha y de las acciones tomadas para restaurar la seguridad.

Evaluaciones de impacto en el tratamiento de datos personales

- A pesar de que no son obligatorias para los privados en Puerto Rico, se recomienda implementar EIPD y análisis de riesgos. En el caso de las agencias de gobierno, esto es de carácter obligatorio.

Multas por incumplimiento:

En Puerto Rico las multas por incumplimiento son de hasta USD 50.000 por violaciones a la ley local y hasta USD 1.500.000 en el caso que sea una ley federal.



República Dominicana

Republica Dominicana en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley N° 172-13 tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. La Constitución Dominicana garantiza el derecho a la intimidad y al honor personal, y establece los principios mínimos para el tratamiento de datos en su artículo 44.

¿Cuáles son los derechos de los titulares?

- Se reconocen los derechos ARCO: Acceso, Rectificación, Cancelación y Oposición. Además, se permite el derecho a indemnización en caso de sufrir daños y perjuicios y de ejercer la acción judicial de habéas data. Los responsables de datos deberán garantizar el pleno y efectivo ejercicio de los derechos.

¿Qué deberes tiene la empresa?

- Se deberán cumplir con los principios y obligaciones determinadas en la normativa como son el deber de secreto del responsable, adoptar medidas de seguridad necesarias para salvaguardar la información y utilizar los datos para los fines para los cuales fueron recolectados, entre otros.

¿Cómo se deben tratar los datos sensibles?

- Únicamente con el consentimiento expreso y por escrito del titular se podrán tratar datos sensibles. Se exceptúan los datos mantenidos por partidos políticos, sindicatos, y entidades sin fines de lucro cuya finalidad sea política, filosófica, religiosa o sindical. Podrán tratarse datos sensibles en la medida que sean necesarios para la prevención, asistencia o tratamiento de salud.

Encargados de tratamiento de datos personales

- El encargado de tratamiento puede ser un tercero mandatario conforme a las instrucciones del responsable de tratamiento. No existen requerimientos expresos, pero recomendamos celebrar un contrato en el que se establezca el objeto del encargo, duración, finalidad, tipo de datos tratados, categorías de los titulares y derechos y obligaciones de las partes.

¿Se debe contar con un registro de actividades de tratamiento?

- La normativa no regula el RAT. Sin embargo, se recomienda contar con uno ya que permite monitorear y supervisar el tratamiento de datos dentro de las organizaciones, actuando de esa manera como una medida interna de control; especialmente para las Sociedades de Información Crediticia.

Notificación de incidentes de seguridad

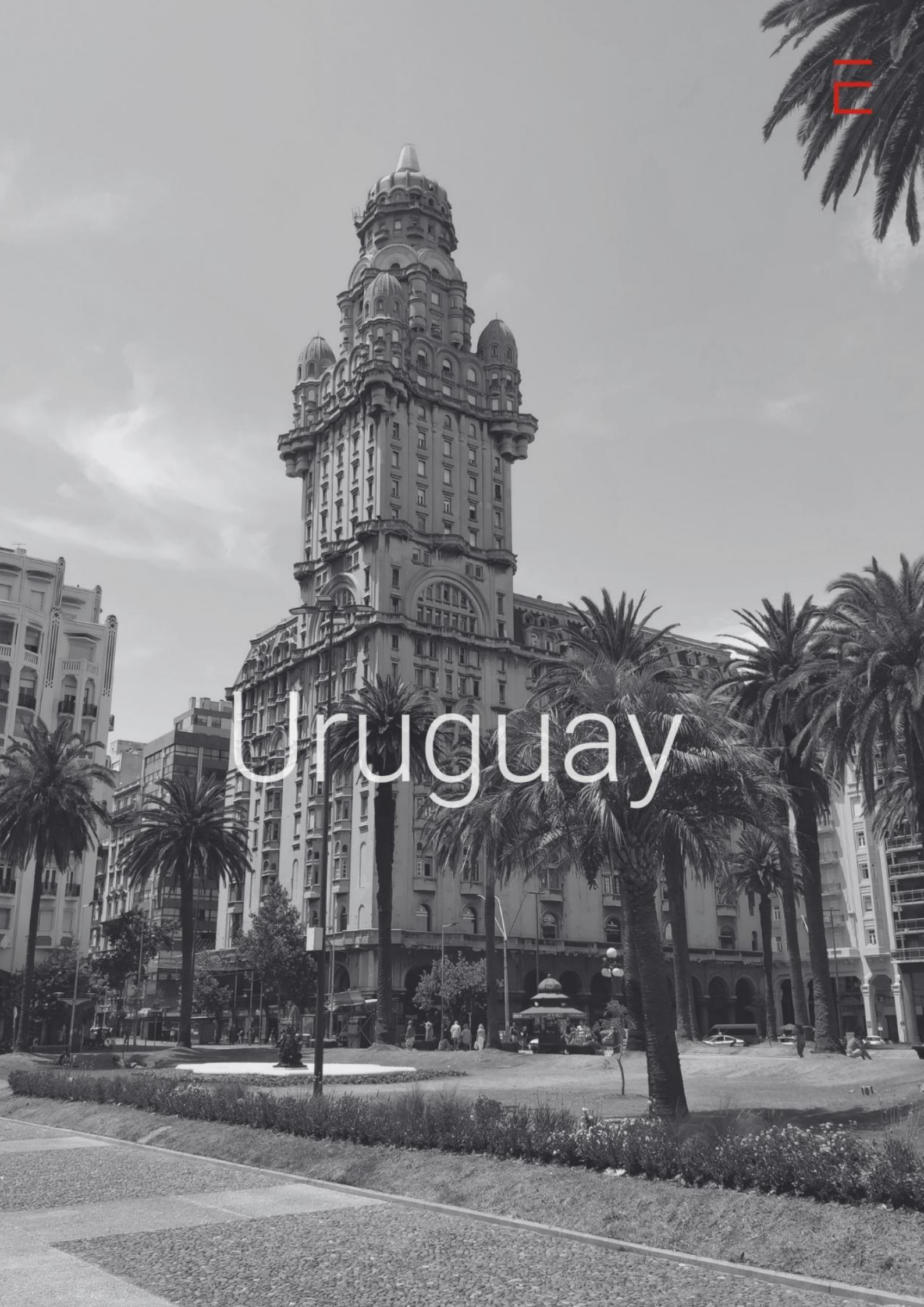
- La normativa actual no define una entidad a la cual notificar las brechas de seguridad que expongan datos personales. De hecho, actualmente no existe una entidad independiente para la protección de datos personales – tipo APDP – en la República Dominicana.

Evaluaciones de impacto en el tratamiento de datos personales

- La ley vigente no regula este asunto. Sin embargo, se recomienda realizar evaluaciones de impacto, de acuerdo con los estándares internacionales, en vistas a cumplir con la responsabilidad proactiva. De igual forma, es recomendable ante cualquier requerimiento regulatorio para transferencia internacional de datos personales en el cual la entidad dominicana es la cedente.

Multas por incumplimiento:

En República Dominicana las multas por incumplimiento son de hasta 150 salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios de derecho común. De igual forma, las personas físicas podrás se sancionadas con prisión correccional de seis meses a dos años. Con la entrada en vigor del Código Penal en el 2026, las personas jurídicas podrán ser responsables por el tipo penal de *"captación y uso no consentido de datos personales".* No obstante, esta norma toma en cuenta la existencia de programas de prevención para la atenuación de la sanción


Uruguay

Uruguay en materia de protección de datos personales:

¿Qué regula la normativa?

- La Ley N° 18.331 del 2008, y sus modificativas establecen el marco legal para la protección de datos personales en Uruguay, tanto para personas físicas como jurídicas. Además, se determina que el derecho a la protección de datos personales es inherente a la persona humana por lo que se comprende en el artículo 72 de la Constitución de la República.

¿Cuáles son los derechos de los titulares?

- Se reconocen en la normativa los derechos de información, acceso, rectificación, actualización, inclusión, comunicación, supresión y de impugnación de valoraciones personales. El responsable deberá dar respuesta en un plazo de 5 días hábiles desde la recepción de la solicitud y debe garantizar canales adecuados y accesibles para el ejercicio de derechos.

¿Qué deberes tiene la empresa?

- Responsables y encargados del tratamiento deben cumplir los principios de protección de datos, aplicar medidas técnicas y organizativas de seguridad, asegurar privacidad desde el diseño y por defecto, gestionar y comunicar incidentes de seguridad, realizar evaluaciones de impacto y designar un delegado de protección de datos en los casos que son obligatorios.

¿Cómo se deben tratar los datos sensibles?

- Los datos sensibles deben tratarse únicamente con el consentimiento expreso y documentado del titular, salvo cuando existan razones de interés general autorizadas por ley, mandato legal del organismo o finalidades científicas o estadísticas con datos disociados. Su almacenamiento está prohibido, excepto en entidades que necesitan estos datos para el cumplimiento de sus fines respecto de sus propios miembros, aunque para comunicarlos o transferirlos siempre se requiere nuevamente el consentimiento expreso y documentado.

Encargados de tratamiento de datos personales

- Según la normativa uruguaya, el encargado de tratamiento es la persona física o jurídica que trata datos personales por cuenta del responsable, conforme a sus instrucciones. La Ley lo define en el artículo 4° y lo distingue del responsable, quien decide sobre la finalidad y los medios del tratamiento.

¿Se debe contar con un registro de actividades de tratamiento?

- Sí. La Ley N.º 18.331 (art. 29 y otros) y el Decreto 414/009 hacen referencia al registro de actividades de tratamiento y determinan quién debe llevarlo. Además de la obligación de inscribir las bases de datos ante la Unidad Reguladora y de Control de Datos Personales (“URCDP”) —incluyendo sus características, categorías de datos, finalidades,

plazos y medidas de seguridad— la normativa también exige la inscripción de los códigos de conducta cuando corresponda.

Notificación de incidentes de seguridad

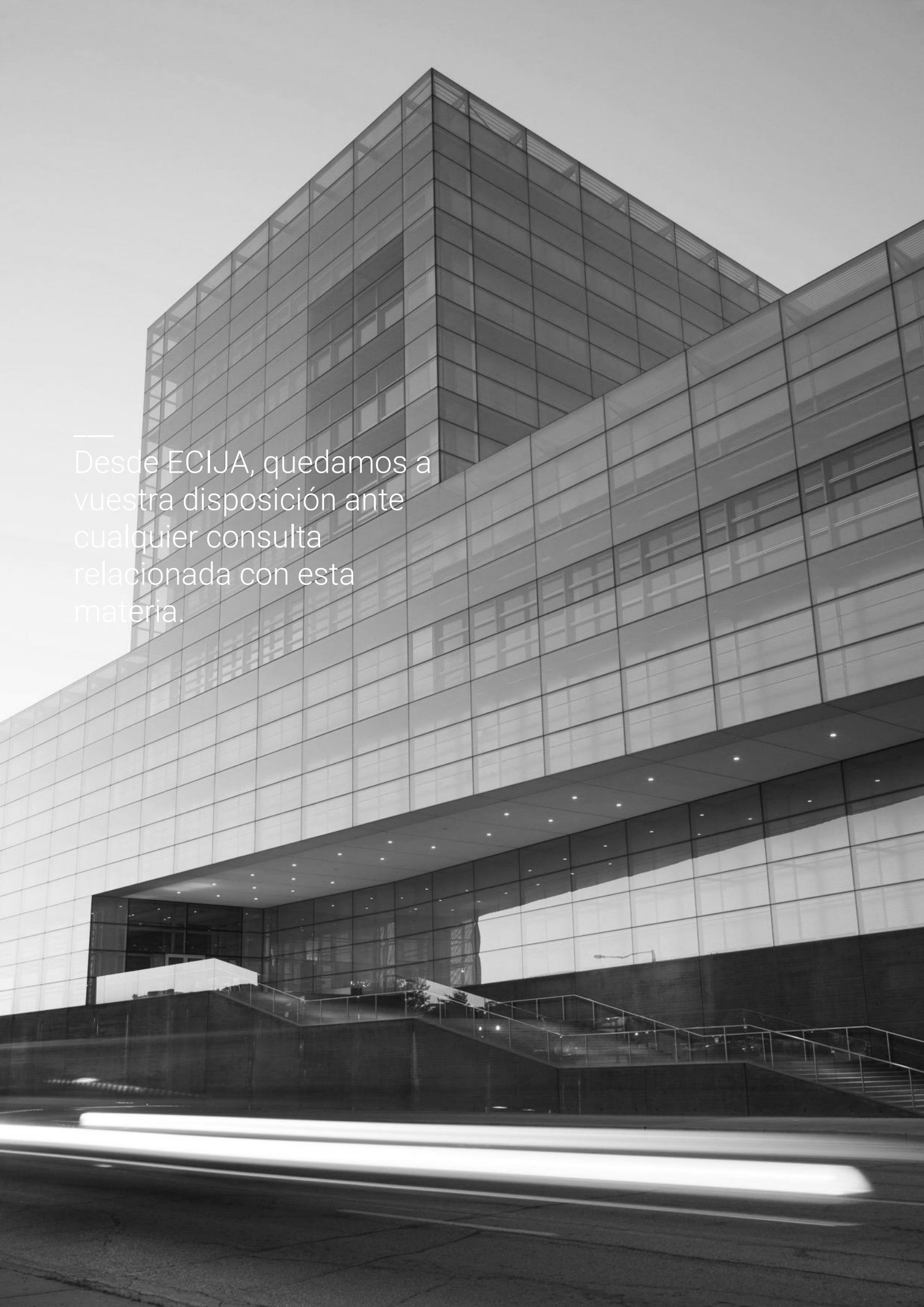
- El responsable o encargado debe notificar a la URCDP cualquier violación de seguridad dentro de las 72 horas, explicando el incidente y las medidas adoptadas para mitigarlo. Una vez resuelto, debe enviar una segunda comunicación informando la solución. Además, cuando la vulneración afecte a titulares, debe notificarles directamente. La URCDP analiza el caso y, si corresponde, lo deriva al Centro Nacional de Respuesta a Incidentes de Seguridad Informática.

Evaluaciones de impacto en el tratamiento de datos personales

- Las EIPD no son obligatorias para todos, pero sí para los casos previstos en el art. 6 del Decreto 64/020. Además, desde la modificación introducida por la Ley 19.924, toda recolección de datos biométricos requiere realizar una EIPD de manera obligatoria.

Multas por incumplimiento:

En Uruguay las multas por incumplimiento alcanzan hasta las 500.000 unidades indexadas (~USD 85.000 aproximadamente). Pueden también aplicarse sanciones como suspensión y clausura de bases de datos.



Desde ECIJA, quedamos a vuestra disposición ante cualquier consulta relacionada con esta materia.