POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

1. INFORMACIÓN GENERAL

Estas políticas corresponden a la empresa FABELJO SAC, identificada con RUC N° 20607618144, con domicilio en Calle Talara N° 222, distrito de Punta Hermosa, provincia y departamento de Lima.

2. OBJETO

La presente política tiene por objeto establecer nuestro compromiso con la protección de datos personales, así como los lineamientos bajo los cuales realizamos el tratamiento de los mismos en el ejercicio de nuestras actividades comerciales, la finalidad para la que lo hacemos, así como los procedimientos mediante los cuales los titulares de los datos puedan ejercer los derechos de acceso, rectificación, cancelación, oposición y demás previstos en la Normativa de Protección de Datos Personales.

3. MARCO NORMATIVO

Como parte de nuestra actividad, tratamos datos personales en cumplimiento con lo dispuesto en la Constitución Política del Perú, en la Ley N° 29733 (Ley de Protección de Datos Personales), su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, y sus normas complementarias y modificatorias.

4. DEFINICIONES

- **Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados (Ejm: Nombre, domicilio, firma, voz, etc).

- **Datos sensibles:** Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad. (Ejm: datos biométricos, origen racial o étnico, ingresos económicos, información relacionada a la salud, etc).

- **Tratamiento de datos personales:** Es cualquier operación o proceso, automatizado o manual, que se realiza sobre los datos personales, tales como recopilación, grabación, registro, almacenamiento, conservación, uso, consulta, transferencia, modificación, supresión, bloqueo, entre otros.

- **Consentimiento:** El consentimiento para el tratamiento de datos personales es la autorización que debe brindar el titular para que sus datos puedan ser recopilados y tratados según la finalidad previamente informada. La autorización puede brindarse de forma verbal o escrita; no obstante, para el tratamiento de datos sensibles es indispensable el consentimiento escrito.

- **Banco de Datos Personales (BDP):** El banco de datos personales es el conjunto organizado de datos de carácter personal, que se pueden encontrar en distintos soportes tales como físicos, magnéticos, digitales, ópticos, entre otros.
- **Titular del Banco de Datos Personales:** El titular del banco de datos personales es aquella persona natural, persona jurídica privada o entidad pública que establece la finalidad para la recopilación y almacenamiento de los datos personales, así como el tratamiento y las medidas de seguridad que le serán aplicables.

- **Encargado del Banco de Datos Personales:** El encargado del tratamiento de datos personales es aquella persona natural o jurídica, pública o privada, que realiza el tratamiento de los datos en nombre y por cuenta del titular del banco de datos. En caso realice tratamiento ajeno a la finalidad del encargo, podrá asumir responsabilidades.

- **Titular de los Datos Personales:** Es aquella persona respecto de la cual se han recopilado datos; y en ese sentido, tendrá un abanico de derechos que podrá ejercer.

- **Derechos ARCO:** Son los derechos que tiene el titular de datos personales frente al titular del banco de datos o al encargado del tratamiento de sus datos. Los derechos ARCO se ejercen personal y gratuitamente a través de solicitudes dirigidas al titular del banco de datos o al encargado del tratamiento. La solicitud de acceso deberá ser atendida dentro de los 20 días siguientes a su presentación, mientras que la de rectificación, cancelación y oposición, en el plazo de 10 días.

- **Flujo transfronterizo:** El flujo transfronterizo consiste en la transferencia de datos personales hacia un destinatario que se encuentra en un país distinto del país de envío, cualquiera sea el soporte en que se encuentren, los medios utilizados para su transferencia o el tratamiento que reciban.

5. FINALIDAD DEL TRATAMIENTO DE DATOS PERSONALES

Nuestra empresa realiza el tratamiento de datos personales de: colaboradores y clientes/usuarios.

Por ello, nuestra empresa tratará dicha información conforme a la normativa vigente, con la finalidad de ejecutar toda y cualquier clase de relaciones jurídicas existentes y/o que puedan existir entre los titulares de los datos y nosotros, sean de carácter comercial, laboral, civil y/o de cualquier otra índole, así como para fines promocionales y/o cualquier otra finalidad lícita debidamente informada a los dichos titulares de datos personales.

6. PRINCIPIOS APLICABLES AL USO DE DATOS PERSONALES

Nos comprometemos a respetar los principios rectores establecidos en la normativa referente a la Protección de Datos Personales. Los cuales son:

- **Principio de legalidad:** El tratamiento de los datos personales se hace conforme a lo establecido en la ley, estando prohibida la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
- **Principio de consentimiento:** Para el tratamiento de los datos personales debe mediar el consentimiento del titular.
- **Principio de finalidad:** Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita, y su tratamiento no debe extenderse a otra finalidad distinta a la aquella para la cual fueron recopiladas.
- **Principio de proporcionalidad:** El tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para los que estos hubieran sido recopilados.
- **Principio de calidad:** Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizada, necesaria, pertinente y adecuada respecto de la finalidad para la que fueron recopilados.
- **Principio de seguridad:** El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.
- **Principio de disposición de recurso:** El titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos cuando estos sean vulnerados por el tratamiento de sus datos personales.
- **Principio de nivel de protección adecuado:** Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a los previsto por la Ley de Protección de Datos Personales o por los estándares internacionales en la materia.

7. OBLIGACIONES DEL TITULAR Y DEL ENCARGADO DE DATOS PERSONALES

En ese sentido, las obligaciones que recaen frente a nuestra empresa (titular) y a los encargados de los bancos de datos serán las siguientes:

- Efectuar el tratamiento de datos personales sólo si el titular ha dado un consentimiento válido.
- No recopilar datos personales de forma fraudulenta, desleal o ilícita.
- Recopilar sólo aquellos datos que sean necesarios para alcanzar la finalidad previamente informada al titular.
- No utilizar los datos personales para finalidades distintas, salvo procedimiento de anonimización o disociación.
- No limitar el ejercicio de los derechos del titular de datos personales.

- Sustituir o complementar los datos personales cuando estos sean inexactos o incompletos.
- Eliminar aquellos datos personales que han dejado de ser necesarios o se haya vencido el plazo para su tratamiento.
- Proporcionar a la Autoridad Nacional de Protección de Datos Personales la información que requiera sobre el tratamiento de datos y el acceso a los bancos.
- Tanto la empresa como el encargado de dar tratamiento de datos personales deberán efectuar dicho tratamiento en observancia de las medidas de seguridad establecidas en el numeral 12 del presente documento.

8. CONSENTIMIENTO

Nuestra empresa requiere del consentimiento libre, previo, expreso, inequívoco e informado del titular de los datos personales para el tratamiento de estos, salvo en los casos de excepción expresamente establecidos por Ley.

En ese sentido, no se requiere consentimiento para el tratamiento de datos personales obtenidos de fuentes accesibles al público, gratuitas o no. Asimismo, podrá tratar sus datos personales de fuentes públicas, conforme al Art. 17° del Reglamento de la Ley de Protección de Datos Personales.

9. TRANSFERENCIA DE DATOS PERSONALES

Para cumplir la finalidad prevista en la presente Política de tratamiento de datos personales, nuestra empresa podrá transferir, a nivel local e internacional, datos personales a empresas que formen parte de un grupo empresarial, ya se trate de empresas existentes o que se creen en el futuro.

En adición, podremos transferir los datos personales a las autoridades policiales, fiscales, tributarias, aduaneras, judiciales, comisiones investigadoras y demás entidades públicas legalmente facultadas conforme a ley, sea en cumplimiento de la normatividad vigente y/o por requerimiento de éstas.

10. DERECHOS DEL TITULAR DE DATOS PERSONALES

En base a la Ley de Protección de Datos Personales, nuestra empresa identifica expresamente que los titulares de datos personales tienen los siguientes derechos:

- **Acceso:** Toda persona tiene derecho a conocer qué información sobre sí misma ha sido almacenada en un banco de datos público o privado; cómo y por qué fue recopilada; así como las transferencias realizadas o las que se prevén realizar.
- **Rectificación:** Toda persona tiene derecho a solicitar la modificación de los datos que fueron recopilados errónea, incompleta, inexacta, desactualizada o falsamente, en banco de datos público o privado. A su vez, permite la actualización e inclusión de nuevos datos personales.
- **Cancelación:** Toda persona puede requerir la cancelación o supresión de sus datos, cuando ya no cumplan una finalidad, cuando se haya revocado el consentimiento o haya transcurrido el plazo para su tratamiento.
- **Oposición:** Toda persona puede oponerse al tratamiento de sus datos personales almacenados en banco público o privado.

Sin embargo, además de los Derechos ARCO, los titulares de datos personales tienen otros derechos, tales como el **derecho de información** (información respecto del tratamiento de sus datos, así como sobre la finalidad, los destinatarios, el banco en el que se almacenarán, el tiempo de conservación y lo relacionado con el tratamiento), el **derecho a la tutela** ante la autoridad, entre otros más.

11. PROCEDIMIENTO PARA EL EJERCICIO DE DERECHOS

Los titulares podrán ejercer sus derechos (por ejemplo: revocar su consentimiento) enviando una solicitud y/o consulta al correo electrónico: contacto@miexperiencia.pe

El titular de los datos personales deberá adjuntar su DNI u otro documento oficial de identidad. En caso de que el titular del dato personal requiera ejercer sus derechos mediante un representante, éste deberá presentar una carta poder legalizada por notario público que lo faculte como tal y su documento de identidad.

12. MEDIDAS DE SEGURIDAD

12.1. CONDICIONES DE SEGURIDAD

12.1.1. CONDICIONES DE SEGURIDAD EXTERNAS

- Adecuación al marco legal apropiado, así como el conocimiento y conciencia de la importancia de la protección de los datos personales.

12.1.2. CONDICIONES DE SEGURIDAD INTERNAS

- Compromiso de nuestra empresa (titular de bancos de datos personales), para brindar los recursos y dirección en la protección de los datos personales.
- Comprender el contexto institucional en el tratamiento y protección de los datos personales (Contexto organizativo, tecnológico, jurídico, legal, contractual, regulatorio, físico, etc.).
- Determinar claramente las responsabilidades y roles organizacionales apropiados con la suficiente autoridad y recursos para liderar y hacer cumplir la política de seguridad para la protección de datos personales.
- Enfoque de gestión del riesgo de los datos personales contenidos o destinados a ser contenidos en los bancos de datos personales.

12.2. TIPOS DE MEDIDAS

En cumplimiento de la normativa vigente, adoptamos medidas de seguridad organizativas, jurídicas y técnicas, las cuales son de obligatorio cumplimiento para aquellos que realicen cualquier tipo de tratamiento de datos personales, tal y como se describe a continuación:

12.2.1. MEDIDAS ORGANIZATIVAS

- Desarrollar una estructura organizacional con roles y responsabilidades de acuerdo con la proporcionalidad de los datos a proteger.
- Llevar un control y registro de los operadores con acceso al banco de datos personales con el objetivo de poder identificar al personal con acceso en determinado momento.
- Revisar periódicamente la efectividad de las medidas de seguridad adoptadas y registrar dicha verificación en un documento adjunto al banco de datos personales.
- Desarrollar procedimientos documentados adecuados para el tratamiento de datos personales.
- Desarrollar un programa de creación de conciencia y entrenamiento en materia de protección de datos personales.
- Desarrollar un procedimiento de auditoría respecto de las medidas de seguridad implementadas, teniendo como mínimo una auditoría anual.
- Desarrollar un procedimiento de gestión de incidentes para la protección de datos personales.

12.2.2. MEDIDAS JURÍDICAS

- Es compromiso de nuestra empresa mantener los formatos de consentimiento para el tratamiento de datos personales, adecuados y de conformidad con la finalidad para la cual son acopiados.
- Por otro lado, nos comprometemos a realizar una adecuación de los contratos del personal relacionado con el tratamiento de datos personales, así como de los contratos con terceros, a través de una cláusula específica de protección de datos personales.

12.2.3. MEDIDAS TÉCNICAS

Es nuestra obligación controlar la asignación y el uso de las contraseñas de los usuarios de los sistemas de información que realizan tratamiento de datos personales, lo cual se logrará mediante la adopción de las siguientes medidas:

- Solicitar a los usuarios que mantengan en secreto las contraseñas asignadas.
- Cuando se utilice un servidor de autenticación, éste debe almacenar las contraseñas de manera cifrada.

- Permitir que el usuario cambie la contraseña asignada cuando lo considere necesario.
- Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un carácter especial.
- Cuando el acceso al sistema esté expuesto en entornos públicos (intranet, internet o similares), se debe bloquear al usuario luego de cinco (05) intentos fallidos de autenticación consecutivos.

En adición, se revisará periódicamente que los privilegios de acceso a los datos personales correspondan al personal autorizado. Esta revisión debe generar un registro de revisión que evidencie la realización de dicha revisión.

El periodo de revisión depende de las políticas organizacionales y el tipo de datos personales que contenga el banco de datos personales. Esta debe realizarse por lo menos semestralmente.

Por otro lado, en caso de bancos de datos no automatizados / físicos, se brindará protección contra el acceso físico no autorizado a través de mecanismos de bloqueo físico, limitando el acceso solo a los involucrados en el tratamiento de datos personales debidamente autorizados. Dichas medidas son las siguientes:

- Se ubicará el banco de datos personales en un gabinete, caja, cajón de un mueble, gaveta o similar siempre y cuando tenga una cerradura con llave o similar, la cual será responsabilidad del operador del banco de datos personales.
- Cuando se contengan datos sensibles, se ubicará el banco de datos personales en un ambiente aislado protegido por cerradura o similar mecanismo, donde la responsabilidad del mecanismo de acceso recae en el titular del banco de datos personales o un responsable delegado por el titular del banco de datos personales.

Por último, se identificarán los accesos realizados a los datos personales para su tratamiento a través de la implementación de un registro de accesos al banco de datos personales, el cual debe contener al menos los siguientes campos:

- Fecha y hora del acceso.
- Persona o personas que realizan el acceso.
- Identificador del titular de los datos personales a tratar
- Motivo del acceso.