THE BIODIVERSITY CONSULTANCY

**THE BIODIVERSITY CONSULTANCY LIMITED**

**LEY DE PROTECCIÓN DE DATOS**

**Abril 2018**

## 1. INTRODUCCIÓN

1.1 La Empresa mantiene datos personales sobre candidatos a puestos de trabajo, empleados, clientes, proveedores y otros individuos para diversos propósitos del negocio.

1.2 Esta ley describe cómo la Empresa pretende proteger los datos personales para asegurar que los empleados entienden las reglas que gobiernan el uso de los datos a los que tienen acceso durante su trabajo.

1.3 Específicamente, la ley requiere que los empleados se aseguran de que el Director General sea consultado antes de que se inicie cualquier nueva actividad de procesamiento de datos para asegurar que los pasos de conformidad necesarios hayan sido tomados.

1.4 El Director General es responsable de la supervisión e implementación de esta ley. Si tiene cualquier duda sobre los contenidos de esta ley o cualquier otro comentario deberá contactar con el/la Gerente de Protección de Datos y el/la Gerente de Recursos Humanos & Comunicación.

## 2. ALCANCE

2.1 Esta ley se aplica a todos los empleados y contratistas, que para este propósito incluye empleados, trabajadores temporales y de agencia, otros contratistas, trabajadores en prácticas y voluntarios/as.

2.2 Todos los empleados y contratistas deben estar familiarizados con esta ley y cumplir con sus condiciones.

2.3 Esta ley completa y apoya las demás leyes de la Empresa.

2.4 La Empresa puede complementar o modificar esta ley mediante políticas y guías adicionales en determinadas ocasiones. Cualquier ley nueva o modificada será enviada a todos los empleados antes de su adopción.

## 3. DEFINICIONES

En esta ley:

"propósito de negocio" significa los fines para los cuales los datos personales puedan ser utilizados por la Empresa, por ejemplo, datos de empleados, datos

administrativos, financieros, regulatorios, datos sobre sueldos, uso de datos para el desarrollo empresarial y datos de salud y seguridad laboral;

"datos personales" significa la información relacionada con individuos identificables, por ejemplo, sobre solicitudes a puestos de trabajo, empleados actuales y del pasado, agencias, empleados bajo contratos temporales o autónomos, clientes, suministradores y contactos de marketing. Esto incluye expresiones de opinión sobre el individuo y cualquier indicación sobre las intenciones de otra persona haca un individuo;

"datos sensibles" significa datos personales que revelan información racial o étnica, opiniones políticas, creencias de tipo religioso o similar, afiliación sindical o comisiones obreras (o no-afiliación), condición o salud mental y/o física, información sobre vida sexual, ofensas criminales, o procedimientos relacionados. Cualquier uso de datos personales confidenciales debe ser controlado de manera estricta de acuerdo con esta ley;

"procesamiento o tratamiento de datos" significa obtener, grabar, guardar o realizar cualquier actividad con los datos, tal como su organización, utilización, modificación, extracción, compartirlos o eliminarlos

## 4. PRINCIPIOS GENERALES

4.1 La política de Empresa es procesar datos personales de individuos de acuerdo con los derechos y leyes de protección de datos pertinentes, como se enumeran a continuación. Todos los empleados son personalmente responsables de la aplicación práctica de la ley de protección de datos de la Empresa.

4.2 La Empresa cumplirá los siguientes principios con respecto al procesamiento de datos personales:

(a) Procesar datos personales de manera justa y legal de acuerdo con los derechos del individuo;

(b) asegurarse de que los datos personales procesados por una razón específica sean adecuados, relevantes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido;

(c) mantener los datos personales precisos y actualizados;

(d) no mantener datos personales durante más tiempo de lo necesario;

(e) mantener los datos personales seguros ante la pérdida o el mal uso;

(f) no transferir datos personales fuera del EEE (Espacio Económico Europeo) (que incluye los Países de la UE, Noruega, Islandia, y Liechtenstein) sin la protección adecuada.

## 5. PROCESAMIENTO JUSTO Y LEGAL

Generalmente, los empleados no deberán procesar datos personales a no ser que:

(a) el individuo a quien pertenezcan los datos haya dado su consentimiento;

(b) el procesamiento sea necesario para llevar a cabo las obligaciones legales o ejercer derechos legales de la Empresa, o

(c) el procesamiento es de otra manera de interés legítimo para la Empresa y no perjudica excesivamente la privacidad del individuo.

5.2 Cuando se estén reuniendo datos personales o estableciendo nuevas actividades de protección de datos, los empleados deberán asegurarse de que los individuos a los que pertenecen los datos procesados reciban la información apropiada sobre protección de datos para conocer cómo serán usados los datos. Existen excepciones a este requisito de notificación. Ante cualquier caso de incertidumbre sobre si se debe o no notificar al individuo, los empleados deben contactar con el/la Gerente de Recursos Humanos y Comunicaciones y el/la Gerente de Protección de Datos.

5.3 Normalmente, será necesario el consentimiento explícito de un individuo para procesar 'datos sensibles', a no ser que existan circunstancias excepcionales o que el procesamiento sea necesario para cumplir con requisitos legales. El consentimiento debe ser informado, lo cual quiere decir que tiene que identificar los datos relevantes, por qué están siendo procesados, y a quien serán relevados. Los empleados deberán contactar con el/la Gerente de Protección de Datos y el/la Gerente de Recursos Humanos & Comunicación para más información sobre cómo conseguir el consentimiento para procesar datos personas sensibles.

## 6. PRECISIÓN, ADECUACIÓN, RELEVANCIA Y PROPORCIONALIDAD

6.1 Los empleados deberán asegurarse de que los datos procesados por ellos sean precisos, adecuados, relevantes y proporcionales al propósito para el cual se obtuvieron. Los datos personales obtenidos para un propósito generalmente no deberán ser utilizados para propósitos no-relacionados a no ser que el individuo haya dado su consentimiento o de otra forma esperase que los datos fuesen a utilizarse de este modo.

6.2 Los individuos pueden pedir a la Empresa que corrija sus datos personales cuando consideren que son imprecisos. Si un empleado recibe tal petición y no está de acuerdo en que los datos personales retenidos son imprecisos, deberán de todas formas anotar la disputa e informar al Gerente de Recursos Humanos y Comunicaciones y Gerente de Protección de Datos

6.3 Los empleados deben asegurarse de que los datos personales mantenidos por la Empresa relacionados con ellos sean precisos y estén actualizados, como sea necesario. Si los detalles personales o circunstancias cambian, los empleados deberán informar al Gerente de Recursos Humanos y Comunicaciones y Gerente de Protección de Datos para que los registros de la Empresa sean actualizados.

## 7. SEGURIDAD

Los empleados deberán mantener sus datos personales seguros ante la pérdida o mal uso. Los datos personales no deben ser compartidos con terceras personas a no ser que sea necesario de acuerdo con los principios de protección de datos. Cuando

la Empresa utilice organizaciones externas para procesar datos personales de su parte, deberán implementarse medidas de seguridad a través de un contrato con las organizaciones para salvaguardar la seguridad de los datos personales. Los empleados deberán consultar con su Gerente de Recursos Humanos y Comunicaciones y Gerente de Protección de Datos para discutir los pasos necesarios para asegurar el cumplimiento de la normativa cuando se establezca cualquier nuevo acuerdo o se altere un acuerdo existente.

## 8. PROCESADORES DE DATOS

Cuando cualquier dato personal que tengamos a nuestro cargo sea transferido o compartido a terceros de nuestra parte, esto debe ocurrir únicamente cuando nos hayamos asegurado de la idoneidad de tales terceros y tengamos un acuerdo formal establecido. Tales acuerdos deben ser aprobados por el/la Gerente de Recursos Humanos y Comunicaciones y el/la Gerente de Protección de Datos.

## 9. RETENCIÓN DE DATOS

Los datos personales no deben ser retenidos más tiempo del necesario. El periodo de tiempo durante el cual los datos deben ser retenidos dependerá de las circunstancias incluyendo las razones por las cuales los datos personales fueron obtenidos.

## 10. TRANSFERENCIA INTERNACIONAL

Los empleados no deberán transferir datos personales de forma internacional sin antes consultar con el/la Gerente de Recursos Humanos y Comunicaciones y el/la e Gerente de Protección de Datos. Existen restricciones sobre las transferencias internacional de datos personales del Reino Unido a otros países, debido a la necesidad de asegurarse de que existen suficientes y adecuadas salvaguardas para protejer los datos personales. Los empleados que estén inseguros sobre los acuerdos existentes o necesarios para atender a éstas condiciones deberán ponerse en contacto con el/la Gerente de Recursos Humanos y Comunicaciones y el/la Gerente de Protección de Datos.

Derechos del individuo

10.1 Los individuos tienen derecho (salvo en determinadas ocasiones) a pedir acceso a información sobre ellos mismos. Tales peticiones deberán referirse de inmediato al Gerente de Recursos Humanos y Comunicaciones y Gerente de Protección de Datos. Esto es especialmente importante porque le Empresa deberá responder a una petición valida dentro de los tiempos legalmente establecidos.

10.2 Cualquier empleado que desee corregir o pedir información propia que la Empresa guarde deberá contactar con el/la Gerente de Recursos Humanos y Comunicaciones y el/la Gerente de Protección de Datos. Debe subrayarse que existen ciertas restricciones sobre la información a la que los individuos tienen derecho bajo la ley pertinente.

10.3 Los empleados no deberán enviar material electrónico sobre marketing directamente (por ejemplo, por correo electrónico) a no ser que hayan recibido el deseo de recibir tales notificaciones. Los empleados deberán atenerse a cualquier petición de un individuo a no utilizar sus datos personales para propósitos directos de marketing y deberán notificar al gerente de Protección de Datos sobre cualquier tal petición. Los empleados deberán contactar con el/la Gerente de Protección de Datos y el/la Gerente de Recursos Humanos y Comunicación para pedir consejo sobre marketing directo antes de comenzar cualquier actividad nueva de marketing directo.

## 11. INFORMAR SOBRE INFRACCIONES

Los empleados tienen la obligación de avisar inmediatamente sobre fallos en el cumplimiento del reglamento de protección de datos, actual o potencial, al Director General, Gerente de Recursos Humanos y Comunicación, y Gerente de Protección de Datos en cuanto han sido identificados. Esto permite a la Empresa:

(a) Investigar el fallo y tomar pasos para remediarlo si fuese necesario; y

(b) Preparar los informes pertinentes para la Comisión de información, y otros. Tenemos un periodo de tiempo corto para generar tales informes.

## 12. CONSECUENCIAS DEL INCUMPLIMIENTO

12.1 La Empresa se toma muy en serio el cumplimiento de esta ley. El incumplimiento pone bajo riesgo a los empleados y le Empresa. La importancia de esta ley significa que el incumplimiento de cualquiera de los requisitos puede conllevar acción disciplinaria, que puede resultar en despido.

12.2 Los empleados con cualquier duda o preocupación sobre cualquier elemento de esta ley no duden en discutirlo con el/la Gestor de Protección de Datos.

Gerente de Recursos Humanos y Comunicación: Katherin Pertsinidis, katherin@thebiodiversityconsultancy.com

Gerente de Protección de Datos: Amelia Topham, amelia.topham@thebiodiversityconsultancy.com

Director General: David Tassell, david.tassell@thebiodiversityconsultancy.com