Política de Confidencialidad y Datos personales

1. Introducción

En Reportability asumimos con seriedad la protección de la información confidencial y los datos personales a los que accedemos en el ejercicio de nuestros servicios. Esta política tiene por objeto establecer las directrices y principios que rigen el tratamiento, uso, protección y confidencialidad de toda información entregada por nuestros clientes y partes interesadas, ya sea de carácter técnico, comercial, estratégico o personal.

2. Alcance

Esta política aplica a todos los colaboradores de Reportability, así como a cualquier tercero que acceda a información por razón de su vinculación con la empresa. Incluye todo tipo de información revelada por clientes a través de medios escritos, electrónicos, visuales o verbales.

3. Información confidencial

Se entenderá por información confidencial toda aquella a la que se acceda en el contexto de los servicios prestados y que no sea de dominio público, incluyendo, pero no limitándose a: estrategias de sostenibilidad, datos financieros, documentos legales, bases de datos, diagnósticos, metodologías, planes de negocios, proyecciones, informes de brechas, datos de trabajadores o personas relacionadas a nuestros clientes.

4. Compromiso de confidencialidad

Toda persona vinculada a Reportability se obliga a no revelar, divulgar o utilizar indebidamente la información confidencial a la que tenga acceso. Dicha información será utilizada exclusivamente para el cumplimiento de los servicios contratados por los clientes y deberá ser protegida con el máximo cuidado. Cualquier acceso, reproducción o difusión de información deberá contar con la autorización expresa de Reportability y estar sujeta a acuerdos formales previos.

5. Excepciones a la confidencialidad

No se considerará confidencial aquella información que sea de dominio público, haya sido conocida con anterioridad a la relación contractual o sea requerida legalmente por una autoridad competente. En tal caso, deberá informarse inmediatamente a Reportability para adoptar las medidas necesarias.

6. Datos personales

6.1 Reportability recolecta y trata datos personales de conformidad con la legislación vigente en Chile y los principios de licitud, finalidad, proporcionalidad y seguridad. Los datos personales de clientes, colaboradores o terceros serán almacenados de forma segura, utilizados únicamente para fines específicos autorizados y nunca compartidos sin consentimiento.

6.2 Sin perjuicio de lo anterior, Reportabilitity declara que no solicita, recolecta ni trata datos personales de clientes o terceros para la prestación de sus servicios de reportes y consultorías en sostenibilidad. Los entregables de Reportability se elaboran con información anonimizada o de carácter público/organizacional.

7. Prohibiciones

7.1 Queda prohibido a cualquier colaborador solicitar o almacenar datos personales de clientes o terceros en el marco de proyectos, salvo que exista una excepción autorizada en los términos de lo dispuesto en el numeral 8vo de este instrumento.

7.2 Cualquier solicitud interna para obtener datos personales, o recepción accidental de ellos como planillas con RUT, datos de salud, datos de RR.HH. u cualquier documento similar que contenga información sensible i debe reportarse inmediatamente al director del proyecto de que se trate y en su defecto, informarlo en un plazo no superior a 24 horas al correo contacto@reportability.cl

7.3 La empresa investigará, contendrá y, si corresponde, eliminará o anonimizará el material recibido, dejando registro del hecho y sus medidas correctivas. No se aplicarán represalias contra quien reporte de buena fe.

8. Excepciones controladas

Si, excepcionalmente, un cliente solicita incluir datos personales (p. ej., testimonios nominales, fotografías de personas, listados nominales en un entregable Reportability, aceptará dicho encargo siempre que:

a) Existir una base legal válida, ya sea consentimiento explícito del titular o fundamento legal aplicable.

b) Se firmará un anexo de tratamiento de datos (DPA) que defina roles de los responsables, la finalidad y plazos de conservación.

e) La información deberá alojarse solo en herramientas aprobadas y con controles de acceso (MFA, cifrado en tránsito y en reposo).

En estos casos excepcionales, Reportability estará siempre al principio de minimazación y de limitación de la finalidad, por lo que solo procesará los datos personales que sean estrictamente necesarios para cumplir con los fines específicos, explícitos y legítimos para los que fueron recolectados y sólo serán utilizados únicamente para los fines para los que fueron obtenidos y que han sido previamente informados al titular.

Al término del proyecto o al vencer la finalidad, los datos personales se eliminarán o anonimizarán, dejando constancia.

9. Datos personales de manejo interno

Con relación a los datos personales internos de Reportability, tales como nómina, remuneraciones, contacto, cumplimiento contractual y de contacto comercial y aquellos estrictamente necesarios para gestión laboral, administrativa y comercial éstos se tratarán bajo los principios de licitud, finalidad, proporcionalidad y seguridad, con acceso restringido y medidas de protección acordes al riesgo.

10. Devolución y eliminación de la información

Toda información, ya sea confidencial o no, deberá ser eliminada una vez finalizados los servicios, dentro del plazo que defina Reportability. La información seguirá siendo propiedad de Reportability o del cliente que la haya entregado.

11. Vigencia del compromiso

Esta política será aplicable durante toda la relación profesional con Reportability y se mantendrá vigente por un período de tres años posteriores al término de dicha relación respecto a la información confidencial a la que se haya tenido acceso.

12. Canal de denuncias y protección al denunciante

12.1 Reportability dispone de un canal confidencial de denuncias para recibir y gestionar, de buena fe, comunicaciones sobre:

a) Presuntas vulneraciones a esta política;

b) Solicitudes o intentos de obtención de datos personales contrarias a la sección 8 excepciones

c) Recepción accidental de datos personales;

d) Incidentes de seguridad o filtraciones; uso indebido o divulgación no autorizada de información confidencial.

12.2 Pueden denunciar colaboradores, ex-colaboradores, proveedores, clientes y cualquier tercero relacionado con los servicios de Reportability

12.3 Las denuncias se podrán efectuar en el correo contacto@reportability.cl con la jefatura directa indistintamente. Se protegerá la identidad del denunciante y la confidencialidad de los antecedentes, permitiendo denuncias anónimas. Está prohibido cualquier tipo de represalia contra quien reporte de buena fe.

12.4 Cuando la denuncia refiera a datos personales, se aplicará contención inmediata (aislar/eliminar datos indebidos, revocar accesos) eliminación o anonimización de la información recibida por error;

13. Procedimiento de gestión de incidentes de seguridad de la información

Para los efectos de esta política, se entiende por *incidente de seguridad* cualquier hecho que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información o de los sistemas de Reportability, incluyendo accesos no autorizados, pérdida o robo de dispositivos, malware, filtraciones, alteraciones no autorizadas de datos o interrupciones relevantes de servicios.

13.1 Cuando una persona detecte o sospeche de un incidente, deberá reportarlo de inmediato a la jefatura o director de proyecto responsable y al soporte técnico a través del correo contacto@reportability.cl, describiendo en términos simples qué ocurrió, cuándo, qué sistema o información se habría visto afectada y qué evidencias preliminares existen (por ejemplo, capturas o mensajes de error). No habrá represalias contra quien reporte de buena fe. Si el hecho involucrara a la jefatura directa de la persona denunciante, el reporte se dirigirá a la Dirección.

13.2 Recibida la alerta, la Dirección o la persona designada abrirá un registro único del incidente y, junto con soporte técnico, realizará una clasificación preliminar dentro de las primeras horas, evaluando alcance e impacto. Para priorizar la respuesta, se considerará crítico todo evento con indicios de fuga de información confidencial o

datos personales, indisponibilidad prolongada de servicios esenciales o presencia de ransomware; se considerará alto el acceso indebido sin evidencia de exfiltración o interrupciones acotadas; y medio o bajo los eventos sin impacto confirmado o de carácter preventivo.

13.3 A continuación, se ejecutarán medidas de contención proporcionales a la severidad, privilegiando la inmediatez en casos críticos. La contención puede incluir la revocación y rotación de credenciales, el aislamiento de equipos o servicios, la deshabilitación temporal de enlaces o integraciones y el bloqueo de accesos sospechosos. Estas acciones se documentarán en el registro del incidente, procurando afectar lo menos posible la continuidad operacional.

13.4 Con el incidente contenido, se desarrollará una investigación técnica si es necesaria para determinar causa raíz, alcance real, sistemas y datos comprometidos y cronología de los hechos. Durante esta fase se preservarán los registros y evidencias relevantes, evitando su alteración o eliminación, y se coordinarán las acciones con el o la líder del proyecto afectado, manteniendo la confidencialidad de los antecedentes y el acceso restringido al expediente.

13.5 Si del análisis se desprende que hay afectación a un cliente o a datos personales tratados de manera excepcional, la empresa realizará las notificaciones pertinentes sin dilación indebida, informando de manera clara y verificable qué ocurrió, qué medidas se adoptaron y qué acciones adicionales se recomendarán. Cuando corresponda por contrato o por ley, se evaluará la comunicación a autoridades competentes.

13.6 Concluida la investigación, se procederá a la recuperación y restauración de servicios y datos a partir de respaldos verificados, aplicando controles reforzados para evitar recurrencias (por ejemplo, endurecimiento de configuraciones, cambios de contraseñas y ajustes de permisos). La Dirección aprobará el cierre del incidente sobre la base de un informe que deberá emitirse idealmente dentro de los treinta días hábiles siguientes a su detección, el cual incluirá causa raíz, impacto, medidas ejecutadas, brechas detectadas y un plan de remediación con responsables y plazos.

13.7 Todas las denuncias e incidentes quedarán documentados en un expediente con acceso restringido. Dichos registros se conservarán por el plazo legal o el que sea necesario para fines de auditoría y defensa. La información relativa a incidentes se considera confidencial y no podrá ser divulgada fuera de los canales definidos; cualquier comunicación externa será autorizada por la Dirección.

13.8 Finalmente, la empresa realizará lecciones aprendidas luego de cada incidente y ensayos periódicos del procedimiento para asegurar su efectividad. Todo el personal tiene el deber de colaborar durante la respuesta, cumplir las instrucciones impartidas y participar en las actividades de capacitación que se programen a partir de las mejoras identificadas

13.9 Esta cláusula complementa la Política de Seguridad de la Información y el procedimiento de respuesta a incidentes. En caso de conflicto, prevalecerá la protección de los titulares, la contención del riesgo y el cumplimiento legal.

14. Cumplimiento y Actualización

El incumplimiento de esta política podrá dar lugar a responsabilidades contractuales o legales según proceda de acuerdo a la normativa laboral vigente y será revisada anualmente o cuando ocurran cambios relevantes en los sistemas, procesos o riesgos de seguridad.

Powered by ecert
Firma electrónica avanzada
CARLA LORENA HORTA DEL PICO
2025.08.23 15:36:09 -0400

Carla Horta del P.

Gerente general

Reportability