
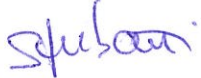
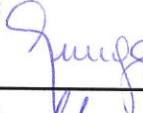




	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

Redactó: Coordinador de Protección de datos	Fecha: 04-05-20	Firma: 
Revisó: Garantía de Calidad	Fecha: 05-05-20	Firma:  Verónica Quiroga Garantía de Calidad Catalysis Argentina S.A.
Revisó: Dirección Técnica	Fecha: 05-05-20	Firma:  Farm. Verónica Padin Directora Técnica Apoderada Catalysis Argentina S.A.
Aprobación: Presidente	Fecha: 06-05-20	Firma:  EMILIO L. JARES FURNO CATALYSIS ARGENTINA S.A. PRESIDENTE
Aprobación Pint Pharma Austria	Fecha:	Firma:

	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

1. Principios

La protección de datos personales es importante para nosotros. Es por eso que procesamos la información personal de nuestros empleados, clientes y socios comerciales conforme a la legislación aplicable en materia de seguridad de datos y protección de datos personales.

Esta política de privacidad (en adelante la “Política”) describe el tipo de información personal que recopilamos, cómo utilizamos esos datos, a quiénes se los transmitimos, y las opciones y derechos que tienen las personas en relación con nuestro procesamiento de datos. Asimismo, se describen las medidas que tomamos para garantizar la seguridad de los datos y cómo los interesados nos pueden contactar si tienen preguntas acerca de nuestras prácticas de privacidad.

Esta guía regula el procesamiento de información en cumplimiento con la protección de datos y las responsabilidades de PINT-PHARMA (representada en el país por Catalysis Argentina S.A). Todos los empleados deben cumplir con la Política.

Esta Política está basada en la Política de Casa Matriz (Data Privacy Policy 01-02-2020) y en la Ley Nacional 25.326

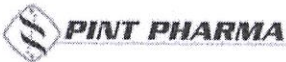

Está dirigida a:

- Las personas o departamentos que toman decisiones acerca de la implementación / provisión de un sistema de aplicación: Departamento de Tecnología de la Información (IT);
- Las personas o departamentos que deciden acerca del uso del sistema para sus tareas;
- El usuario, es decir, aquellos que utilizan el sistema provisto para realizar sus tareas operacionales;
- El personal que, por su actividad, dispone base de datos de pacientes (por ejemplo, Patient Support Program)
- El personal que, por actividad, dispone base de datos de profesionales de la salud.
- El coordinador de protección de datos de la empresa, quien supervisa la implementación del sistema mediante el asesoramiento y el control, y realiza las tareas que le fueron asignadas.

Se aplican los siguientes principios:

>>El software y hardware de procesamiento de datos deben utilizarse para tareas operacionales, para la finalidad prevista y deben ser seguros contra pérdidas y manipulación de datos. Su uso para fines privados requiere de permiso expreso.

En caso de no existir sistema dedicado a tal fin, y se utilice papel como soporte, el responsable debe asegurar la protección de los datos y las consideraciones no varían.

	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

>> Cada empleado es responsable de la implementación de la guía en su área de responsabilidad y deberá monitorear su cumplimiento regularmente.

>> Aquellos responsables del procesamiento de los sistemas utilizados se asegurarán de que los empleados (usuarios) estén informados acerca de esta guía. Esto también aplica a los empleados temporarios.

>> El Coordinador de protección de datos brinda asesoramiento acerca de la implementación de la Política y verifica su cumplimiento. En este aspecto, todos destinatarios de la Política tienen la obligación de proveer información a dicho Coordinador.

2. El Coordinador de protección de datos de la empresa

2.1 Catalysis Argentina S.A ha designado un Coordinador de protección de datos de la empresa. Los datos de contacto del mismo pueden encontrarse en el Anexo I del presente documento.

El Coordinador de protección de datos deberá realizar las tareas que le fueron asignadas por ley y por esta Política, libre de instrucciones y haciendo uso de su experiencia técnica y calificaciones profesionales.

2.2 El Coordinador de protección de datos informa y asesora a la gerencia y a los empleados acerca de sus obligaciones con respecto a la protección de datos. Tiene la responsabilidad de monitorear el cumplimiento con las normas de protección de datos y las políticas del controlador para la protección de datos personales, incluidas la asignación de responsabilidades, concientización y capacitación de los empleados.



En el caso del procesamiento de datos de alto riesgo, el Coordinador de protección de datos asesora a la persona responsable acerca de la evaluación del riesgo.

2.3 El Coordinador de protección de datos reporta directamente a la gerencia de la empresa.

2.4 El Coordinador de protección de datos participará en todos los asuntos de privacidad desde las etapas iniciales y tanto la gerencia de la empresa como los empleados lo asistirán para llevar a cabo sus obligaciones.

2.5 La empresa, a través del Coordinador de protección de datos, lleva un registro de todas las operaciones de procesamiento. La persona responsable de un procesamiento informa esta actividad inmediatamente conforme a las especificaciones estipuladas por el Coordinador de protección de datos. El mismo procedimiento aplica para las solicitudes de cambios. Ante cualquier duda con respecto a la información requerida por ley, se podrá consultar al Coordinador de protección de datos.

Independientemente de esta notificación, cuando se planea la introducción de un nuevo procesamiento o la modificación de procedimientos existentes, se deberá informar al

	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

Coordinador de protección de datos acerca de la finalidad y el contenido de la aplicación y del cumplimiento de la obligación para su notificación. Para las encuestas estandarizadas (cuestionarios, concursos, campos para completar en la página principal en Internet, etc.), se le deberá entregar al Coordinador de protección de datos el cuestionario, etc. para su aprobación.

- 2.6 En caso de ser solicitado, la empresa pondrá a disposición de la autoridad supervisora, en nuestro caso, el Ministerio del Interior, el registro de todas las operaciones de procesamiento,. De acuerdo con la gerencia, el Coordinador de protección de datos será responsable de este tema y trabajará junto con la autoridad supervisora.
- 2.7 Todos los empleados podrán contactar al Coordinador de protección de datos inmediatamente por comentarios, sugerencias o reclamos y, de ser requerido, manteniendo absoluta confidencialidad.

3. Compras / hardware y software

3.1 La adquisición de hardware y software por lo general se lleva a cabo ante la solicitud de la persona / departamento que decide acerca del procesamiento, a través del departamento central de compras de procesamiento de datos. Desde la selección del hardware y el software, el principio de garantía de protección de datos mediante el diseño y configuraciones previas de privacidad amigables es considerado un criterio de apoyo.



3.2 Si con la compra se requiere la incorporación de un nuevo procedimiento para el procesamiento de datos personales, el solicitante deberá informar al Coordinador de protección de datos con anterioridad. La compra se realizará únicamente tras la opinión de dicho Coordinador.

El Coordinador informará acerca de la necesidad de llevar a cabo una evaluación de impacto de la privacidad.

3.3 No se podrá utilizar hardware ni software privado para el procesamiento de datos personales. El uso de hardware y software privado en los hogares y en el extranjero (por ejemplo, computadoras portátiles privadas) requiere la aprobación del departamento de Tecnología de la Información (IT) en cada caso particular.

3.4 El departamento de IT lleva una lista del hardware y los programas de aplicaciones utilizados. El Coordinador de protección de datos puede acceder a estos registros en todo momento.

3.5 Ante la sospecha de robo de hardware y software, acceso a datos personales sin autorización, sabotaje, etc., se deberá informar de inmediato al departamento de IT y al Coordinador de protección de datos.

	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

4. Compromiso / capacitación de empleados

4.1 Todos los empleados que manejen datos personales deberán comprometerse con el manejo confidencial de los mismos y el cumplimiento con esta Política.

Todos los empleados se comprometen mediante la firma del documento “Compromiso con la privacidad de datos y secretos comerciales”. Dicha declaración de compromiso debe ser incluida en los archivos personales.

4.2 Se le debe informar al Coordinador de protección de datos acerca de la contratación de empleados y la ubicación de sus lugares de trabajo para brindarles capacitación adicional y determinar cualquier necesidad de control.

4.3 Para las sesiones de capacitación acordadas junto con la respectiva gerencia departamental, los empleados en cuestión deberán ser liberados de sus trabajos.

5. Transparencia del procesamiento de datos.

5.1 Si el Coordinador de protección de datos determina que el procesamiento previsto se encuentra sujeto a una Evaluación de impacto de privacidad, deberá informarlo de inmediato. El procesamiento entonces podrá llevarse a cabo únicamente con el acuerdo del Coordinador. En caso de dudas, lo decidirá la gerencia.



5.2 Si un interesado hace uso de su derecho de acceso conforme al Art. 14 de la Ley de Protección de datos (Ley 25.326), o de su derecho de rectificación u objeción, el Coordinador de protección de datos procesará los datos de manera central. Las solicitudes de información y de inspecciones hechas por parte de los empleados serán atendidas por el Departamento de Recursos Humanos.

Se deberá garantizar que los datos puedan estar a disposición del interesado, si así lo deseara, en un formato estructurado, de uso común y lectura mecánica.

6. Recopilación/ procesamiento de datos personales

6.1 La recopilación y el procesamiento de datos personales sólo podrá llevarse a cabo en la medida permitida por ley. También se deberán tener en cuenta las condiciones especiales para la recopilación y procesamiento de datos sensibles conforme al Art. 7 de la Ley 25.326). En principio, dicha información sólo se podrá procesar y utilizar cuando sea necesario para el desarrollo de las tareas de la empresa y esté directamente relacionada con los fines del procesamiento.

6.2 Se deberá garantizar que los interesados no sean objeto de una decisión basada únicamente en procesamiento automatizado que tenga efectos legales sobre ellos o los afecte significativamente de manera similar (por ejemplo, perfilamiento).

	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

6.3 Con anterioridad a la incorporación de nuevas finalidades para la recopilación de datos personales, a fin de determinar la admisibilidad, el controlador de la aplicación deberá documentar por escrito el uso previsto de los datos. En principio, sólo estará permitido un cambio en la finalidad si el procesamiento es compatible con aquellos fines para los cuales los datos fueron recopilados originalmente. Los criterios de ponderación utilizados en el curso de dicho cambio serán analizados individualmente.

Asimismo, se deberá documentar el análisis para llevar las constancias correspondientes.

También se permitirán cambios en la finalidad si las personas a cargo consiguen el consentimiento del interesado. Al mismo tiempo, antes de la recopilación o almacenamiento de datos, el controlador deberá especificar por escrito si se debe cumplir con la obligación legal de notificar a la persona en cuestión y de qué manera.

6.4 Si organismos solicitan información acerca de los interesados, sólo podrán recibir esta información sin el consentimiento de los mismos, de haber una obligación legal o un interés legítimo de la empresa que justifique dicha transferencia, y si se establece la identidad inequívoca del solicitante. Ante cualquier duda, se deberá contactar al Coordinador de protección de datos.

7. Almacenamiento / transferencia / eliminación de datos



7.1 El almacenamiento de datos se lleva a cabo básicamente en la nube y en las unidades de discos de la red provistos para este fin. En cuanto a las redes, el departamento de IT tiene la responsabilidad de hacer copias de seguridad de los datos almacenados en el servidor.

7.2 En la medida en que se requiera almacenar datos en distintas ubicaciones por razones técnicas (por ejemplo, computadoras portátiles, de escritorio), el usuario será el responsable de hacer la copia de seguridad de dichos datos. De poder acceder a la red (por ejemplo, mediante una Tablet, computadora portátil con red de área local inalámbrica (WLAN), etc.), se deberá transferir la base de datos vigente a la unidad de disco de la red reservada para el usuario, al menos una vez por semana. Las medidas de protección de datos seleccionada deberán documentarse en el registro de actividades de procesamiento.

7.3 La persona encargada del procesamiento de datos deberá cumplir con los períodos y fechas legales de retención y eliminación de datos. Se deberá informar al departamento de IT acerca del cumplimiento con las fechas límite, particularmente con respecto a la eliminación de datos personales en las copias de seguridad.

7.4 Al transferir o devolver componentes de IT que no fueran necesarios, el usuario tiene la obligación de asegurarse de que todos los datos hayan sido eliminados efectivamente.

8. Proveedores de servicios externos / procesamiento de datos / mantenimiento



	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

Ante la contratación de proveedores de servicios externos por primera vez para el procesamiento de datos personales o pasos del procesamiento individuales (por ejemplo, recopilación, eliminación = deshecho) o para actividades (por ejemplo, de mantenimiento, reparación) mediante los cuales se pudiera tener conocimiento de datos personales, se deberá informar al Coordinador de protección de datos al respecto. A su vez, se deberá presentar al Coordinador de protección de datos un contrato borrador de cumplimiento con los requisitos del Art 28 del Reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y los criterios de control del procesamiento de datos llevados a cabo o previsto subsiguientemente.

9. Rendición de cuentas y documentación

El cumplimiento con los requisitos que surgen de esta guía deberá ser verificable en todo momento (“Rendición de cuentas”). En particular, se deberá proporcionar constancias mediante documentación entendible y conclusiva por escrito respecto de las medidas tomadas y las consideraciones relacionadas.

Anualmente, se informará a Presidencia, un resumen de las actividades en referencia a las actividades de Protección de Datos y un resumen de los Desvíos o no conformidades detectados en dicho periodo, junto con un Plan de Mejoras.

	POLÍTICA DE PRIVACIDAD DE DATOS	
Versión 1		

ANEXO I: Coordinador de protección de datos

Sabrina Iubatti

Office: +54 11 4730 2539

Mobile: +54 9 11 6525 7704

Email: sabrina.iubatti@pint-pharma.com