

POLÍTICA GLOBAL

PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Esta política señala los requisitos para asegurarse de que cumplamos nuestro compromiso de proteger la información de personas obtenida durante nuestras actividades de negocios asegurando altos estándares de protección a nivel mundial.

La información de personas, es aquella que puede ser utilizada para identificar personas o individuos vivos. (Empleados, clientes, accionistas, empleados de proveedores y maquiladores y participantes de estudios clínicos).

¿A QUIÉN APLICA ESTA POLÍTICA?



A todos los empleados que manejen información de personas como parte de su labor.








Gerentes que son responsables de asegurarse que los controles adecuados estén establecidos.



Para cumplir con esta Política, se espera que todas las áreas SET sigan las normas y procedimientos globales o que sus normas y procedimientos locales vayan de acuerdo a esta política.

PRINCIPIOS CLAVE

-  Debemos proteger la información de personas recolectada, registrada, almacenada, alterada, recuperada, revelada, compartida, combinada, respaldada, destruida o utilizada durante el curso de nuestras actividades de negocio.
-  Cada área SET establecerá claramente las responsabilidades y la rendición de cuentas por la custodia de la información de personas que maneja.
-  Por lo menos una persona por área SET / funcional (“Líder en Privacidad”) será designada y rendirá cuentas por el desarrollo e implementación de controles, consistentes con los objetivos de esta política, de acuerdo al tipo de información de personas que esa área SET / funcional maneje. El líder se apoya en un representante de la oficina global de privacidad.
-  Las políticas, normas y procedimientos de las áreas locales SET / funcional deben de reflejar requisitos legales y de regulación más estrictos que los enunciados en esta política. Cuando este sea el caso, estos requisitos deberán cumplirse.
-  El uso eficiente de la información de personas que la Compañía procesa, requiere que las áreas SET / funcional cooperen entre sí para asegurar el balance óptimo entre las necesidades locales y/o las específicas y el beneficio general de la Compañía. Esto derivará en la imposición de requisitos más estrictos que los que las leyes locales establezcan.




NORMAS Y PROCEDIMIENTOS DOCUMENTADOS

Cada área SET, apoyada por un representante de la Oficina Mundial de Privacidad, deberá desarrollar e implementar políticas, normas y procedimientos que describan la conducta que se

debe asumir para regir el manejo de la información de personas que procesa de acuerdo con esta política y la regulación local aplicable.

TRANSPARENCIA

Los “líderes” deberán implementar procedimientos en sus áreas SET para asegurarse que:

-  Cuando sea legalmente necesario, los sujetos deben recibir o hacer accesible para ellos un aviso sobre la información que la compañía procesa sobre ellos.
 - > El aviso de la Compañía debe proporcionar la información de la filial de AstraZeneca que este recopilando o utilizando la información y describir los usos que se le dan a esta, incluyendo si será compartida o discutida con terceros, afiliados locales o extranjeros. Cuando sea legalmente necesario, también deberán describir las facultades de los sujetos para acceder a la información de personas y borrar o corregir cualquier dato inexacto.
 - > La Compañía solo procesará información de personas por la vía descrita en el aviso y/o cualquier declaración de privacidad asociada (Ej. Guías electrónicas de privacidad) o para los propósitos, inherentes de tal descripción o que son obvios para el sujeto.
 - > La Compañía puede utilizar información de personas para propósitos no declarados en el aviso, donde se han identificado previamente los datos.
-  La Compañía solo reunirá la cantidad necesaria de información de personas para satisfacer su razón de negocios, recursos humanos, científicos, legales y/o propósitos regulatorios.
-  Cuando la Compañía compre información sobre individuos a terceros con reputación en el manejo y control de la misma (Ej. Listas de vendedores), se debe informar al individuo que estamos procesando su información.

Como parte de la prestación de servicios de SI/TI a nuestro personal, terceros y afiliados, los sistemas de la Compañía registran automáticamente el manejo de la información de personas respecto a la utilización de los sistemas (acceso a Internet, llamadas telefónicas). A menos que esté legalmente permitido este tipo de información no debe ser vista o utilizada de manera continua o rutinaria. Sin embargo, cuando la ley lo permita, esta información será utilizada para facilitar el cumplimiento de nuestras obligaciones legales y regulatorias y/o establecer, ejercer o defender nuestros derechos legales (y otros propósitos asociados).

INFORMACIÓN PRIVILEGIADA DE PERSONAS.

Los líderes deben implementar políticas, normas y/o procedimientos dentro de su área SET para asegurarse que, cuando sea legalmente necesario, solo procesemos información privilegiada de personas clasificada como tal (cuentas bancarias, número de pasaporte, información sobre la salud, número del seguro social o de la tarjeta de crédito), si contamos con su conocimiento. Los líderes deben mantener procedimientos para registrar y evidenciar que el consentimiento se obtuvo. La clasificación predeterminada de la Compañía para información privilegiada es “Estrictamente Confidencial”.

DISPOSITIVOS PORTÁTILES DE ALMACENAMIENTO DE DATOS.

El personal debe encriptar la información de personas temporalmente almacenada en dispositivos portátiles (memorias USB, memory sticks, CD's, DVD's y tarjetas de memoria flash) y protegerla con una contraseña. Los dispositivos portátiles solo deberán ser utilizados para almacenar información de personas por periodos cortos de tiempo en donde no se tenga acceso a métodos más seguros de transmitirla y exista una razón válida de negocio para ello. Los dispositivos portátiles que contengan dicha información deberán ser entregados de manera personal o a través de un mensajero seguro, no es aceptable enviarlos a través del servicio postal, nacional o internacional. A la brevedad posible y después de que la transferencia se haya completado la información de personas deberá ser borrada de ese dispositivo, e incluso y de ser necesario se deberá destruir el dispositivo con la información.

Nunca se deberá guardar la información de personas en dispositivos que no pertenezcan a la Compañía (computadoras personales), tampoco se deberá guardar en dispositivos portátiles para facilitar el acceso en dispositivos que no pertenezcan a la Compañía. Nunca se deberá enviar información de personas a través de cuentas de correo electrónico personales como Hotmail.

Para mayor información vea: "Utilizar WinZip para proteger la información de AZ"


ACTIVIDADES PROMOCIONALES Y DE MERCADOTECNIA



En algunos mercados, la Compañía envía comunicados de mercadotecnia directamente a los consumidores vía correo electrónico, teléfono y mensajes de texto (SMS). En la mayoría de los mercados, también se envía material promocional a los profesionales de la salud a través de estos medios. Si es un requisito legal, los líderes deberán tener políticas, normas y/o procedimientos para asegurarse de que dichos comunicados sean enviados con el consentimiento previo del individuo. Un mecanismo de cancelación deberá ser incluido en cada comunicado (darse de baja del servicio en el correo electrónico) o deberá estar disponible para el individuo. Se deben mantener las listas de los consumidores y profesionales de la salud que han optado por rechazar el servicio.

ACCESO, EXACTITUD, CORRECCIÓN Y RETENCIÓN

Cuando sea un requisito legal, los líderes deberán implementar procedimientos dentro de sus áreas SET para asegurarse de que la compañía provea a los individuos acceso a su información. Cuando este legalmente permitido, la Compañía puede cobrar una cuota para garantizar el acceso.

Los líderes deberán asegurarse que todas las áreas SET tenga procedimientos para asegurarse de que la información de personas que procesa sea:

-  Compartida solamente con terceros que sean socios, parte de su personal o proveedores que tengan el derecho, o una necesidad legítima, de verla. Terceros estarán obligados, por contrato, a implementar las medidas organizacionales y tecnológicas necesarias para proteger la integridad y confidencialidad de la información de personas mientras esté en su poder.

-  Corregida, si los individuos contactan a la Compañía y lo solicitan, y se debe mantener actualizada.
-  Eliminada una vez que el propósito para el que fue requerida se ha satisfecho, a menos que sea conservada para cumplir con un requerimiento legal, regulatorio o alguna política. La información eliminada puede ser recuperada de dispositivos de respaldo por un tiempo mientras se elimina permanentemente.

Para mayor información vea la política mundial que aplica a los registros de manejo y las políticas de seguridad del área SET, así como la política de manejo de archivos y registros y la sección de seguridad de la información de la política mundial de protección de los activos y recursos de la Compañía.

COMPARTIR INFORMACIÓN DE PERSONAS

La Compañía puede compartir o revelar información de personas en atención a ordenamientos de carácter legal, regulatorios, gubernamentales o solicitudes de aplicación de la ley, o cuando este dentro de su legítimo interés y sea legalmente permitido hacerlo (venta o fusión de negocio).

De acuerdo con muchas organizaciones internacionales, el uso eficiente de nuestros SI/TI involucra desplazar la información de personas que procesamos por nuestra red, compartirla y revelarla a nuestras filiales alrededor del mundo y terceros aprobados. La Compañía debe usar las medidas organizacionales y tecnológicas apropiadas para proteger la integridad y confidencialidad de la información de personas conforme se desplaza por nuestra red.

ENTRENAMIENTO

Cualquier entrenamiento realizado por el líder del área SET incluirá un elemento de protección de datos y un elemento de alerta de la privacidad de la información, adecuados para las actividades que procesa dicha área SET. Los materiales de alerta de la privacidad de la información serán desarrollados en conjunto con un representante de la Oficina Mundial de Privacidad.

RIESGO

En consulta con el representante de la Oficina Global de Privacidad, el líder se debe asegurar que el registro de riesgos de su área SET refleje de manera precisa la protección de información y los riesgos de privacidad que corren por su área de negocios, y que los planes de remediación apropiados existen para la gestión/eliminación de estos.

Para mayor información vea la Política Mundial de Protección de los Activos y Recursos de la Compañía.