Política de protección de datos de PBI

Aprobado por:	Consejo Internacional y Consejo Internacional Operativo
Fecha de aprobación:	25 Marzo 2021
Autor:	Comité Jurídico
Última revisión:	25 Marzo 2021
Próxima revisión:	Marzo 2023
Se aplica a:	Todas las personas empleadas, voluntarias y consultoras de PBI.

Propósito

Una protección de datos potente es esencial para el disfrute del derecho a la privacidad. Como organización basada en los derechos humanos, PBI se compromete a ser transparente sobre cómo recopila y utiliza los datos personales de cada persona, así como a cumplir sus obligaciones de protección de datos en línea según el Reglamento General de Protección de Datos (RGPD) de la UE. Esta política establece el compromiso de PBI con la protección de datos, así como los derechos y obligaciones individuales respecto a los datos personales.

Esta política se aplica a los datos personales del quienes forman o han formado parte del personal de PBI (como contratistas o en puestos asalariados, voluntarios o pasantes), o han solicitado un empleo, que se denominarán «datos personales relacionados con recursos humanos». Esta política no se aplica a los datos personales de clientes ni a otros datos personales tratados con fines operativos.

PBI ha asignado el rol de responsable de protección de datos al puesto de Coordinación de Gobernanza. Su papel es informar y asesorar a PBI sobre cuáles son las obligaciones de la organización respecto a la protección de datos. Es responsabilidad del Consejo Internacional evaluar los riesgos relacionados con la protección de datos y tomar medidas que mitiguen dichos riesgos. La dirección de contacto de la persona responsable de protección de datos es governance@peacebrigades.org. Las preguntas o solicitudes de información adicional sobre esta política deben dirigirse a la persona responsable de protección de datos.

Definiciones

Por «datos personales» se entiende cualquier información relacionada con una persona viva que pueda ser identificada a partir de dicha información. Por «tratamiento» se entiende cualquier uso que se haga de esos datos, lo que incluye recopilarlos, almacenarlos, enmendarlos, revelarlos o destruirlos.

Por «categorías especiales de datos personales» se entiende información sobre la racialización o etnia de origen de una persona, sus opiniones políticas, convicciones religiosas o filosóficas, afiliación a un sindicato, salud, vida u orientación sexual y datos genéticos o biométricos.

Por «datos sobre antecedentes penales» se entiende información sobre las condenas e infracciones penales de una persona, así como la información relativa a las acusaciones y litigios penales.

Principios de protección de datos

PBI trata los datos personales relacionados con los recursos humanos de acuerdo con los siguientes principios de protección de datos:

- PBI trata datos personales de forma legal, justa y transparente.
- PBI recopila datos personales únicamente para fines específicos, explícitos y legítimos.
- PBI trata datos personales solo si es adecuado, pertinente y se limita a lo necesario para los fines de dicho tratamiento.
- PBI mantiene la exactitud de los datos personales que trata y toma todas las medidas razonables para garantizar que los datos personales inexactos se rectifican o se eliminan sin demora.
- PBI conserva datos personales solo durante el tiempo en que sea necesario tratarlos, como indica su Política de Conservación de Documentos.
- PBI adopta las medidas adecuadas para garantizar que los datos personales están seguros y protegidos contra el tratamiento no autorizado o ilegal, así como contra su pérdida, destrucción o daño accidentales.

PBI, en sus avisos de privacidad, informa a cada persona sobre los motivos del tratamiento de sus datos personales, el uso que se hace de ellos y la base legal del tratamiento. PBI no tratará datos personales de personas por ningún otro motivo. Cuando PBI invoque sus intereses legítimos como base para el tratamiento de los datos, llevará a cabo una evaluación para garantizar que dichos intereses no se vean invalidados por los derechos y libertades de las personas.

En los casos en los que PBI trata categorías especiales de datos personales o datos sobre antecedentes penales, ya sea para cumplir con sus obligaciones legales o ejercer sus derechos según la legislación laboral, este tratamiento se hace según su política sobre categorías especiales de datos y datos de antecedentes penales.

PBI actualizará los datos personales relacionados con recursos humanos con prontitud si una persona advierte a la organización de que sus datos han cambiado o no son los correctos.

Los datos personales recopilados durante la relación laboral, de contratista, voluntariado, aprendizaje o prácticas, se conservan en el expediente personal de cada individuo (en formato impreso, electrónico, o en ambos), y en los sistemas de Recursos Humanos. Los períodos durante los cuales PBI conserva datos personales relacionados con recursos humanos figuran en sus avisos de privacidad a los individuos.

El registro que mantiene PBI de sus actividades de tratamiento de datos personales relacionados con recursos humanos cumple con los requisitos del Reglamento General de Protección de Datos (RGPD).

Derechos individuales

Cada individuo, como persona interesada, tiene una serie de derechos respecto a sus datos personales.

Solicitudes de acceso de la persona interesada

Las personas interesadas tienen derecho a presentar una solicitud de acceso. Si una persona realiza una solicitud de acceso a sus propios datos, PBI le comunicará:

- si existe o no tratamiento de esos datos, y si es el caso, qué categorías de datos personales son, y el origen de los mismos si estos datos no se hubieran recopilado directamente de la persona en cuestión;
- a quiénes se han revelado o podrían revelarse sus datos, incluidos los destinatarios que estén fuera del Espacio Económico Europeo (EEE), además de las salvaguardias que se aplican a dichas transferencias de datos;
- durante cuánto tiempo se guardan sus datos personales (y cómo se decide dicha duración);
- sus derechos de rectificación o supresión de datos, o de restricción u oposición al tratamiento;
- que si considera que PBI no ha respetado sus derechos en materia de protección de datos tiene derecho a reclamar ante la Autoridad Belga de Protección de Datos; y
- si PBI toma decisiones automatizadas o no, y cuál es la lógica de dicha toma de decisiones;
- si PBI va a destruir los datos cuando haya pasado un tiempo.

PBI también proporcionará a la persona interesada una copia de los datos personales que se estén tratando. En circunstancias normales se entregarán en formato electrónico si la persona ha hecho su solicitud por vía electrónica, a menos que esté de acuerdo con otro método.

Si la persona solicitante desea más copias, PBI cobrará una tarifa basada en el costo administrativo que supone para PBI suministrar de dichas copias adicionales.

Para pedir acceso a sus datos personales, la persona interesada debe enviar una solicitud a governance@peacebrigades.org. Es posible que sea necesario en algunos casos que PBI pida a la persona interesada un documento de identidad antes de tramitar la solicitud. PBI informará a cada solicitante si necesita verificar su identidad y qué documentos son necesarios para ello.

En circunstancias normales, PBI responderá a cada solicitud en el plazo de un mes natural a partir de la fecha de recepción. En ciertos casos, como por ejemplo si PBI trata grandes cantidades de datos sobre la persona concreta, el plazo de respuesta puede ser de tres meses naturales a partir de la fecha de recepción de la solicitud. Si se da esta última circunstancia, PBI informará de ello por escrito a la persona interesada en el plazo de un mes natural a partir de la recepción de la solicitud original.

PBI no tiene la obligación de responder a solicitudes de acceso que estén manifiestamente infundadas,, o sean vejatorias o excesivas. Como alternativa, PBI puede aceptar responder pero cobrará una tarifa basada en el coste administrativo de responder a la solicitud. Es probable que una solicitud de acceso de la persona interesada sea manifiestamente infundada o excesiva si dicha persona repite una solicitud a la que PBI ya ha respondido. Si una persona presentase una solicitud infundada, vejatoria o excesiva, PBI le notificará que es así, además de si responderá o no a la misma.

Otros derechos

Las personas tienen otros derechos relacionados con sus datos personales. Pueden exigir a PBI que:

- rectifique los datos inexactos;
- deje de tratar los datos, o borre los que ya no sean necesarios para los fines del tratamiento;
- deje de tratar sus datos o los borre, si sus intereses individuales prevalecen sobre los motivos legítimos que tenga PBI para tratar sus datos (en los casos en los que PBI base su tratamiento de datos en los intereses legítimos de la organización);
- deje de tratar los datos o los elimine si dicho tratamiento es ilegal; y

- deje de tratar los datos durante un periodo, si los datos son inexactos o si estuviese en disputa que sus intereses individuales prevalecen o no sobre los motivos legítimos que tenga PBI para tratar los datos.

Para pedir a PBI que tome alguna de estas medidas, la persona interesada debe enviar una solicitud a governance@peacebrigades.org.

Seguridad de los datos

PBI se toma muy en serio la seguridad de los datos personales relacionados con los recursos humanos. PBI cuenta con políticas y sistemas de control internos para proteger los datos personales de su pérdida, destrucción accidental, mal uso o divulgación, y para garantizar que no se accede a los datos, excepto por parte de la plantilla de PBI en el apropiado desempeño de sus obligaciones.

En los casos en que PBI implica a terceros para que en su nombre traten datos personales, se les proporcionan instrucciones escritas, tienen el deber de confidencialidad y la obligación de aplicar las medidas técnicas y organizativas pertinentes, de modo que quede garantizada la seguridad de los datos.

Evaluaciones de impacto

Algunos de los tratamientos que realiza PBI pueden crear riesgos para la privacidad. En los casos en los que el tratamiento suponga un alto riesgo para los derechos y libertades de las personas, PBI llevará a cabo una evaluación de impacto del tratamiento de datos para definir la necesidad y la proporcionalidad de tratarlos. Esto incluirá tener en cuenta para qué fines se lleva a cabo la actividad, cuáles son los riesgos para las personas y qué medidas pueden establecerse para mitigar dichos riesgos.

Violaciones de la seguridad de los datos

Si PBI descubre que ha tenido lugar una violación de la seguridad de los datos personales relacionados con recursos humanos que suponga un riesgo para los derechos y las libertades de las personas, lo comunicará a la Autoridad Belga de Protección de Datos en un plazo de 72 horas desde su descubrimiento. PBI registrará todas las violaciones de seguridad de los datos con independencia del efecto que tengan.

Cuando sea probable que la infracción resulte en un alto riesgo para los derechos y libertades de las personas, PBI comunicará a las personas afectadas que se ha producido dicha infracción y les informará tanto de sus posibles consecuencias como de las medidas de reducción del riesgo que haya adoptado.

Transferencias internacionales de datos

Los datos personales relacionados con los recursos humanos se transfieren a servidores situados en el Reino Unido para su tratamiento, y es posible que se transfieran a otros países fuera del EEE. Los datos se transfieren fuera del EEE de acuerdo con una Decisión de Adecuación o de Cláusulas Contractuales Tipo para datos entre países de la UE y de fuera de la UE, que se haya firmado con el ente procesador de datos.

Responsabilidades individuales

Son las personas físicas las responsables de asistir a PBI a mantener sus datos personales actualizados. Es responsabilidad individual informar a PBI sobre cambios en los datos proporcionados a la organización; por ejemplo, si alguien se muda de casa o cambian sus datos bancarios.

Es posible que durante el trascurso de su empleo, contrato, periodo de voluntariado, prácticas o aprendizaje haya personas pueden tener acceso a los datos personales de otros individuos. En este caso, PBI confía en que cada persona colaborará en el cumplimiento de sus obligaciones en materia de protección de datos con respecto al personal, los voluntarios y otras personas.

Las personas que tienen acceso a datos personales tienen las siguientes obligaciones:

- acceder únicamente a los datos a los que tienen autoridad para acceder y solo para los fines autorizados;
- no divulgar los datos salvo a personas que tengan la autorización correspondiente (tanto de dentro como de fuera de PBI);
- mantener la seguridad de los datos (por ejemplo: cumpliendo las normas de acceso a los locales y los ordenadores, lo que incluye protegerlos con contraseña, así como el almacenar y destruir los archivos de forma segura);
- no sacar ni datos personales, ni dispositivos que los contengan o puedan utilizarse para acceder a datos personales, de los locales de PBI sin adoptar las medidas de seguridad adecuadas (como el cifrado o la protección con contraseña) para proteger los datos y el dispositivo;
- no almacenar datos personales en unidades locales o en dispositivos personales que usen para fines laborales; y
- comunicar inmediatamente a la persona responsable de protección de datos las violaciones de la seguridad de los datos de las que obtengan conocimiento.

Véase la Política de seguridad de datos de PBI para más detalles sobre los procedimientos de seguridad de PBI.

El incumplimiento de estos requisitos puede constituir una infracción disciplinaria, que se tratará según el procedimiento disciplinario de PBI. Las infracciones significativas o deliberadas de esta política, como por ejemplo el acceso a los datos de la plantilla sin autorización previa o sin una razón legítima para ello, pueden constituir una falta grave y podrían dar lugar al despido sin previo aviso.

Formación

Como parte del proceso de iniciación y a intervalos regulares a partir de entonces, PBI impartirá formación a todas las personas sobre sus responsabilidades en materia de protección de datos.

Las personas cuyas atribuciones requieran un acceso habitual a datos personales (o que sean responsables de la aplicación de esta política o de responder a las solicitudes de acceso de otros individuos en virtud de la misma) recibirán una formación adicional para ayudarles a comprender cuáles son sus obligaciones y cómo pueden cumplirlas.