Versión 2.0; última actualización: 20 de julio de 2026

1. Finalidad

PECB se compromete a proteger los Datos Personales de sus empleados, clientes, candidatos a la certificación/candidatos certificados, participantes en la capacitación, instructores, auditores, supervisores de exámenes, socios, distribuidores, contratistas, proveedores, usuarios del sitio web y demás personas cuyos Datos Personales procesa.

Esta Política establece los principios, las responsabilidades y los requisitos de gobernanza aplicables a toda la organización para la recopilación, el uso, la divulgación, el almacenamiento, la transferencia, la conservación y la eliminación de Datos Personales, de manera lícita, leal, transparente, segura y responsable, por parte de PECB o en su nombre.

Su propósito es garantizar que los Datos Personales se procesen de manera lícita, leal, transparente y segura, y de conformidad con las leyes aplicables en materia de protección de datos y privacidad.

2. Alcance

Esta Política se aplica a:

- Todos los empleados, directivos, gerentes, contratistas, consultores, trabajadores temporales y demás personas de PECB que procesen Datos Personales para PECB o en su nombre;
- Los Datos Personales en cualquier formato, incluida la información electrónica, física, verbal, visual o registrada;
- Todos los sistemas, servicios, aplicaciones, plataformas, ubicaciones, entornos de trabajo remoto y entornos de terceros aprobados de PECB; y
- Todos los terceros que procesen Datos Personales en nombre de PECB.

Esta Política se aplica independientemente del lugar en el que se acceda a los Datos Personales, se almacenen, se transfieran o se procesen.

3. Legislación aplicable en materia de protección de datos

PECB debe cumplir con la Ley de Protección de Datos Personales de Singapur de 2012 (PDPA, siglas en inglés) y el Reglamento (UE) 2016/679, el Reglamento General de Protección de Datos (RGPD), incluidas las directrices regulatorias aplicables, siempre que cada marco de trabajo sea aplicable a una actividad de procesamiento de Datos Personales. La PDPA y el RGPD deben considerarse componentes igualmente aplicables del marco de trabajo de protección de datos de PECB para toda la organización, dentro de sus respectivos ámbitos territorial y material.

PECB también debe cumplir con otras leyes aplicables en materia de protección de datos y privacidad en los países y jurisdicciones en los que opera o presta servicios, junto con los requisitos contractuales, de acreditación y regulatorios pertinentes.

Cuando más de una ley de protección de datos sea aplicable a la misma actividad de procesamiento, PECB debe identificar y cumplir los requisitos aplicables en virtud de cada marco de trabajo jurídico pertinente. Cuando dichos requisitos difieran o se solapen, PECB debe implementar las medidas apropiadas para cumplir las obligaciones aplicables pertinentes y debe solicitar asesoramiento al Responsable de Protección de Datos o al Responsable Jurídico cuando sea necesario.

La identidad del responsable del tratamiento de PECB pertinente, junto con los datos de contacto externos actualizados del Responsable de Protección de Datos y, cuando corresponda, del representante de PECB en la Unión Europea, debe estar disponible públicamente.

4. Definiciones

Para esta Política, se aplican las siguientes definiciones:

Datos Personales significa cualquier información relativa a una persona física identificada o identificable, independientemente de que la información sea exacta o no y de que esté registrada en un soporte material o de otro modo.

Procesamiento significa cualquier operación realizada sobre Datos Personales, incluida la recopilación, el registro, la organización, la estructuración, el almacenamiento, la modificación, la recuperación, la consulta, el uso, la divulgación, la transmisión, la restricción, la eliminación, la anonimización o la destrucción.

Titular de los datos significa la persona a la que se refieren los Datos Personales.

Responsable del Tratamiento significa una organización que determina los fines y los medios del procesamiento de Datos Personales.

Encargado del Tratamiento significa una organización que procesa Datos Personales en nombre de un responsable del tratamiento.

Intermediario de Datos significa una organización que procesa Datos Personales en nombre y para los fines de otra organización, según se entiende en la PDPA de Singapur.

Consentimiento significa una manifestación libre, específica, informada e inequívoca mediante la cual una persona acepta el procesamiento de Datos Personales, cuando este criterio sea exigido por la legislación aplicable.

Datos de Categorías Especiales significa Datos Personales que revelan el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, los datos genéticos o biométricos utilizados para la identificación única, la información relativa a la salud o la información relativa a la vida sexual o la orientación sexual de una persona.

Datos Personales Sensibles significa Datos Personales que pueden generar un mayor riesgo para la persona si se accede a ellos, se utilizan o se divulgan de manera indebida, incluidos los documentos de identificación, la información financiera, las credenciales de las cuentas, los registros de exámenes, los resultados de la verificación de sanciones y los Datos de Categorías Especiales.

Violación de Datos Personales significa un incidente de seguridad que da lugar a la destrucción, pérdida o alteración accidental o ilícita de Datos Personales, o a la divulgación o el acceso no autorizados a estos.

Anonimización significa el procesamiento de Datos Personales de manera que la información ya no pueda asociarse a una persona identificable mediante medios razonablemente disponibles.

Seudonimización significa el procesamiento de Datos Personales de manera que no puedan atribuirse a una persona específica sin utilizar información adicional que se conserve por separado y de forma segura.

5. Principios de protección de datos

PECB debe procesar los Datos Personales de acuerdo con los siguientes principios:

Licitud, lealtad y transparencia - los Datos Personales deben procesarse de manera lícita, leal y de una forma que las personas puedan comprender razonablemente.

Limitación de la finalidad - los Datos Personales deben recopilarse, utilizarse y divulgarse únicamente para fines específicos, explícitos, legítimos y razonables. No deben procesarse para una finalidad incompatible, salvo que lo permita la legislación aplicable.

Minimización de datos - solo deben recopilarse y procesarse los Datos Personales que sean adecuados, pertinentes y razonablemente necesarios para la finalidad prevista.

Exactitud - se deben adoptar medidas razonables para garantizar que los Datos Personales sean exactos, completos y se mantengan actualizados cuando sea necesario.

Limitación de la conservación - los Datos Personales no deben conservarse durante más tiempo del necesario para los fines empresariales, contractuales, legales, regulatorios, de acreditación, certificación, quejas, apelaciones, seguridad o probatorios pertinentes.

Integridad y confidencialidad - los Datos Personales deben protegerse mediante medidas técnicas, físicas y organizativas apropiadas y proporcionales a la naturaleza, la sensibilidad y los riesgos del procesamiento.

Responsabilidad proactiva - PECB debe mantener políticas, procedimientos, registros, capacitación, evaluaciones, controles y actividades de seguimiento adecuados para demostrar el cumplimiento de los requisitos aplicables en materia de protección de datos.

6. Gobernanza y responsabilidades

Todos los empleados y contratistas de PECB comparten la responsabilidad de gestionar y proteger adecuadamente los Datos Personales de acuerdo con las funciones que se les hayan asignado y los requisitos aplicables de PECB.

La **Alta dirección** debe:

- Aprobar las políticas importantes;
- Proporcionar los recursos adecuados para el cumplimiento de los requisitos de privacidad y protección de datos;
- Promover una cultura de privacidad, confidencialidad y responsabilidad;
- Garantizar que los riesgos importantes para la privacidad se tengan en cuenta en la toma de decisiones de la organización;
- Respaldar la independencia del Responsable de Protección de Datos; y
- Revisar los riesgos importantes para la privacidad, los incidentes, los hallazgos de auditoría y las acciones correctivas.

El **Responsable de Protección de Datos** debe:

- Informar y asesorar a PECB y a su personal sobre las obligaciones en materia de protección de datos;
- Realizar el seguimiento del cumplimiento de las leyes aplicables en materia de protección de datos, de esta Política y de los procedimientos relacionados;
- Supervisar la implementación del marco de trabajo de gobernanza de la privacidad de PECB;
- Asesorar sobre las Evaluaciones de Impacto relativas a la Protección de Datos y las evaluaciones de riesgos para la privacidad;
- Apoyar la gestión de las solicitudes del Titular de los Datos;
- Apoyar la evaluación, la gestión y la notificación de las Violaciones de Datos Personales;
- Cooperar con las autoridades de supervisión y regulatorias competentes;
- Actuar como punto de contacto para las autoridades y los Titulares de los Datos;
- Apoyar las actividades de capacitación y concienciación sobre privacidad;
- Realizar el seguimiento de las acciones correctivas relacionadas con la privacidad; y
- Informar a la Alta dirección sobre asuntos importantes relacionados con la privacidad.

El Responsable de Protección de Datos debe participar de manera oportuna en los asuntos que impliquen un procesamiento significativo de Datos Personales y debe desempeñar su función con la independencia, los recursos, la confidencialidad y el acceso a la Alta Dirección adecuados.

El **Especialista en Operaciones de Seguridad de la Información** debe:

- Implementar y mantener controles de seguridad adecuados;
- Realizar evaluaciones de riesgos de seguridad de la información;
- Gestionar los controles de identidad, acceso, autenticación, cifrado, seguimiento y seguridad de los dispositivos terminales;
- Apoyar la gestión de vulnerabilidades y las pruebas de seguridad;
- Apoyar la investigación, contención y subsanación de las Violaciones de Datos Personales;
- Mantener registros de los incidentes de seguridad; y
- Informar al Responsable de Protección de Datos y a la Alta Dirección sobre los riesgos importantes para la seguridad.

Los **Gerentes y Responsables de Procesos/Módulos** deben:

- Identificar los Datos Personales que se procesan y la finalidad de su procesamiento;
- Garantizar que se implementen los avisos de privacidad y los mecanismos de consentimiento cuando sea necesario;
- Restringir el acceso a las personas que tengan una necesidad empresarial autorizada;
- Definir los requisitos de acceso;
- Aprobar y revisar periódicamente el acceso de los usuarios;
- Actualizar y aplicar los requisitos aprobados de conservación y eliminación;
- Notificar al Responsable de Protección de Datos antes de introducir actividades de procesamiento o realizar cambios sustanciales en ellas;
- Garantizar que se aborden los riesgos para la privacidad identificados y las acciones correctivas.
- Apoyar la eliminación segura, la anonimización, la exportación y la corrección de los Datos Personales.

Los **Responsables de Contratos encargados de las relaciones con terceros** deben:

- Realizar la debida diligencia adecuada en materia de privacidad y seguridad;

- Garantizar que se implementen las cláusulas contractuales requeridas en materia de protección de datos;
- Consultar al Responsable de Protección de Datos antes de contratar encargados del tratamiento o proveedores de servicios que impliquen un procesamiento significativo de Datos Personales;
- Garantizar que los Datos Personales se devuelvan, transfieran o eliminen de forma segura cuando finalice una relación de prestación de servicios.

Los **empleados y contratistas** deben:

- Procesar los Datos Personales únicamente para fines empresariales autorizados;
- Cumplir esta Política y los procedimientos relacionados;
- Mantener la confidencialidad;
- Utilizar únicamente los sistemas y canales de comunicación aprobados;
- Proteger las credenciales y los derechos de acceso;
- Completar la capacitación requerida en materia de privacidad y seguridad;
- Informar inmediatamente sobre cualquier sospecha de Violación de Datos Personales, divulgación no autorizada o incumplimiento de la Política; y
- Cooperar en las investigaciones, auditorías y acciones correctivas relacionadas con la privacidad.

7. Fundamentos jurídicos, consentimiento y procesamiento permitido

Antes de procesar Datos Personales, PECB debe identificar y documentar la base jurídica aplicable a la actividad de procesamiento en virtud de la legislación pertinente.

PDPA de Singapur

Cuando sea aplicable la PDPA de Singapur, PECB debe recopilar, utilizar o divulgar Datos Personales únicamente:

- Con el consentimiento de la persona;
- Cuando el consentimiento se considere otorgado en virtud de la legislación aplicable;
- Cuando sea aplicable una excepción permitida al consentimiento; o
- Cuando la ley lo autorice o exija de otro modo.

RGPD de la UE

Cuando sea aplicable el RGPD, PECB debe identificar una base jurídica adecuada, que puede incluir:

- El consentimiento del Titular de los Datos;
- La ejecución de un contrato o la aplicación de medidas precontractuales solicitadas por el Titular de los Datos;
- El cumplimiento de una obligación legal;
- La protección de intereses vitales;
- El cumplimiento de una misión realizada en interés público, cuando corresponda; o
- Los intereses legítimos de PECB o los intereses legítimos de un tercero, siempre que sobre dichos intereses no prevalezcan los derechos y las libertades del Titular de los Datos.

Gestión del consentimiento

Cuando se requiera el consentimiento, PECB debe garantizar que este:

- Se obtenga antes de que comience el procesamiento correspondiente;
- Se proporcione mediante un lenguaje claro y comprensible;
- Sea específico para la finalidad correspondiente;
- Se presente por separado de términos no relacionados, cuando corresponda;
- Pueda retirarse; y
- Se modifique cuando la finalidad o la naturaleza del procesamiento cambien sustancialmente.

La retirada del consentimiento no debe afectar al procesamiento que ya se haya realizado lícitamente antes de dicha retirada.

PECB puede continuar con el procesamiento cuando sea aplicable otra base jurídica, obligación legal, requisito contractual, requisito de acreditación o excepción permitida.

8. Recopilación, transparencia y Declaración de Privacidad

PECB debe proporcionar a las personas información clara y accesible sobre cómo se procesan sus Datos Personales.

La Declaración de Privacidad debe incluir, cuando corresponda:

- La identidad y los datos de contacto de la entidad de PECB pertinente;
- Las finalidades para las que se procesan los Datos Personales;
- La base jurídica o autorización legal aplicable;
- Las categorías de Datos Personales procesados;
- Información relativa a los encargados del tratamiento y proveedores de servicios externos;
- Las transferencias internacionales y las garantías aplicables;
- Los periodos de conservación;
- Los derechos de los Titulares de los Datos y las opciones para presentar reclamaciones;

Cuando los Datos Personales se recopilen directamente de la persona, la declaración correspondiente debe proporcionarse en el momento de la recopilación o antes de esta.

9. Requisitos para el tratamiento de datos

9.1. Minimización y exactitud de los datos

- PECB debe limitar la recopilación y el procesamiento de Datos Personales a lo que sea razonablemente necesario para la finalidad correspondiente.
- PECB debe revisar periódicamente los formularios, los campos de las plataformas, las bases de datos, los registros de empleados, los registros de exámenes y certificaciones, los registros de marketing, los registros de auditoría y otros repositorios que contengan Datos Personales.
- La información/los registros que sean innecesarios, excesivos, duplicados o que hayan dejado de ser pertinentes deben eliminarse, anonimizarse o dejar de utilizarse, según corresponda.
- PECB debe proporcionar mecanismos razonables para que las personas puedan revisar, actualizar o corregir sus Datos Personales.

9.2. Datos de Categorías Especiales y Datos Personales Sensibles

PECB debe procesar los Datos de Categorías Especiales, los registros de antecedentes penales, la información relativa a la salud, los documentos de identificación, la información financiera y otros Datos Personales Sensibles únicamente cuando:

- El procesamiento sea necesario para una finalidad definida;
- Se hayan identificado una base jurídica adecuada y cualquier condición adicional requerida;
- La recopilación sea proporcional a la finalidad;
- El acceso se limite específicamente al personal autorizado;
- Se apliquen medidas de protección reforzadas;
- La conservación sea limitada; y
- Se evalúen los riesgos para la privacidad cuando corresponda.

Los Datos Personales Sensibles no deben recopilarse únicamente porque puedan ser útiles en el futuro.

9.3. Datos Personales de menores

Los sitios web y servicios de PECB no están destinados a menores (personas menores de 16 años), y PECB no recopila deliberadamente sus Datos Personales.

Cuando PECB tenga conocimiento de que se han recopilado Datos Personales de un menor sin la autorización requerida, se deben adoptar medidas razonables para restringir, corregir o eliminar la información de conformidad con la legislación aplicable.

10. Privacidad desde el Diseño, Registros y Evaluaciones de Riesgos

Los requisitos de privacidad deben tenerse en cuenta al diseñar, adquirir, desarrollar, implementar o modificar sustancialmente sistemas, servicios, productos, procesos empresariales, herramientas de inteligencia artificial, actividades de seguimiento o verificación, actividades de marketing, procesos relacionados con los empleados y acuerdos con terceros.

De manera predeterminada, PECB debe:

- Recopilar únicamente los Datos Personales necesarios;
- Limitar el acceso según la función y las necesidades empresariales;
- Utilizar configuraciones que protejan la privacidad;
- Limitar la conservación;
- Impedir la disponibilidad sin restricciones de los Datos Personales; y
- Aplicar controles de seguridad adecuados.

10.1. Inventario de Datos Personales y Registro de Actividades de Tratamiento

PECB debe mantener Registro de Actividades de Tratamiento (RAT) que contengan:

- La actividad y el Responsable del Proceso;
- Las categorías de Titulares de los Datos y de Datos Personales;
- Las finalidades del procesamiento y la base jurídica o autorización legal;
- Los sistemas y las ubicaciones utilizados;
- Los destinatarios y los encargados del tratamiento;
- Las transferencias internacionales;
- Los periodos de conservación;
- Las medidas de seguridad;
- Las declaraciones de privacidad pertinentes;
- El procesamiento automatizado.

Los Responsables de Procesos deben notificar al Responsable de Protección de Datos cuando se cree, modifique sustancialmente, transfiera, externalice o interrumpa una actividad de procesamiento.

10.2. Evaluaciones de Riesgos para la Privacidad y EIPD

Se debe realizar una evaluación de riesgos para la privacidad antes de que comience el procesamiento o se modifique sustancialmente cuando la actividad pueda generar un riesgo significativo para las personas.

Cuando sea aplicable el RGPD, se debe realizar una Evaluación de Impacto relativa a la Protección de Datos cuando sea probable que el procesamiento entrañe un alto riesgo para los derechos y las libertades de las personas.

La evaluación puede ser necesaria para:

- El seguimiento sistemático o a gran escala;
- Los Datos de Categorías Especiales o la identificación biométrica;
- La inteligencia artificial, la elaboración de perfiles o la toma de decisiones automatizada;
- El procesamiento que implique a personas vulnerables;
- El procesamiento a gran escala; o
- Las tecnologías nuevas o emergentes.

11. Procesamiento Automatizado, Verificación y Elaboración de Perfiles

Cuando PECB utilice el procesamiento automatizado, la verificación, el seguimiento o la elaboración de perfiles, debe:

- Definir y documentar la finalidad;
- Identificar la base jurídica, el consentimiento o la autorización aplicables;
- Informar a las personas afectadas cuando sea necesario;
- Evaluar la calidad, la pertinencia y la exactitud de la información utilizada;
- Implementar medidas de protección contra resultados incorrectos, injustos o discriminatorios;
- Restringir el acceso a los resultados;
- Establecer periodos de conservación adecuados;
- Proporcionar una revisión humana cuando sea necesario o apropiado; y
- Permitir que las personas cuestionen o impugnen las decisiones cuando corresponda.

Para la verificación en listas de sanciones, PECB debe garantizar que las posibles coincidencias se revisen antes de adoptar medidas desfavorables, que se gestionen los falsos positivos, que se restrinja el acceso y que los resultados se conserven únicamente durante el tiempo necesario.

PECB no debe tomar decisiones basadas únicamente en el procesamiento automatizado que produzcan efectos jurídicos o efectos de importancia similar, salvo que lo permita la legislación aplicable y se cuente con las medidas de protección adecuadas.

12. Derechos de los Titulares de los Datos y Gestión de Solicitudes

Las personas pueden ejercer los derechos que les correspondan en virtud de la legislación aplicable. Dependiendo de la jurisdicción, estos pueden incluir el derecho a:

- Recibir información sobre el procesamiento;
- Acceder a los Datos Personales y obtener una copia;

- Corregir Datos Personales inexactos o incompletos;
- Solicitar la supresión o la restricción;
- Oponerse al procesamiento;
- Recibir los Datos Personales en un formato legible;
- Retirar el consentimiento;
- Obtener garantías con respecto a determinadas decisiones basadas únicamente en el procesamiento automatizado;
- Solicitar la revisión humana de determinadas decisiones automatizadas; y
- Presentar una reclamación ante una autoridad competente.

Estos derechos no son absolutos y pueden estar limitados por las condiciones legales aplicables, las excepciones, las obligaciones de conservación, los requisitos de acreditación o certificación, las reclamaciones legales o los derechos de terceros.

12.1. Presentación de una Solicitud, Pregunta o Reclamación

Las solicitudes habituales para corregir o modificar datos privados pueden enviarse al Servicio de Atención al Cliente de PECB a support@pecb.com o mediante la opción **Enviar una solicitud** del Centro de Ayuda de PECB.

Otras solicitudes, sugerencias o reclamaciones relacionadas con el procesamiento de sus Datos Personales deben dirigirse al Responsable de Protección de Datos a dpo@pecb.com.

De conformidad con el artículo 27 del RGPD, PECB ha designado a un representante en la Unión Europea, ubicado en Lisboa, Portugal. Puede ponerse en contacto con el representante en gdpr.representative@pecb.com.

12.2. Verificación, Tarifas y Plazos

Las personas pueden ejercer los derechos que les correspondan en virtud de la legislación aplicable.

PECB debe:

- Utilizar medidas razonables y proporcionales para verificar la identidad y la autoridad del solicitante;
- Evitar solicitar más Datos Personales de los necesarios para la verificación;
- Gestionar las solicitudes de forma gratuita, salvo que la ley permita cobrar una tarifa (*se aplica una tarifa cuando se presentan múltiples solicitudes de acceso de los Titulares de los Datos (DSAR, siglas en inglés)*);
- Notificar previamente al solicitante si corresponde aplicar una tarifa permitida por la ley;
- Responder sin dilación indebida y dentro del plazo legal aplicable; y
- Informar al solicitante dentro del plazo de respuesta inicial si se requiere una prórroga permitida por la ley.

12.3. Denegación, Limitación y Supresión

Cuando se deniegue o limite una solicitud, PECB debe explicar los motivos, con sujeción a las restricciones legales, e indicar las opciones disponibles para presentar una reclamación o apelación.

PECB puede conservar la información cuya supresión se haya solicitado cuando sea necesario para:

- El cumplimiento de requisitos legales o regulatorios;
- Las obligaciones de certificación o acreditación;
- Las obligaciones contractuales;
- La gestión de reclamaciones y apelaciones;
- La prevención del fraude;
- Las reclamaciones legales;
- Los registros de seguridad, auditoría, financieros o contables; o
- Otra finalidad lícita y documentada.

Antes de eliminar una cuenta o los registros relacionados, PECB debe explicar las consecuencias pertinentes, incluida la posible pérdida de acceso a los registros de certificación, los registros de exámenes, los materiales de capacitación o los servicios.

13. Comunicaciones de Marketing y de Servicio

Cuando sea necesario, PECB debe obtener el consentimiento antes de enviar comunicaciones de marketing sobre cursos de capacitación, boletines informativos, seminarios web, eventos, promociones o servicios relacionados.

Los destinatarios deben poder retirar su consentimiento o darse de baja fácilmente.

PECB puede utilizar los datos de contacto obtenidos a través de una relación existente con un cliente para enviar comunicaciones específicas y pertinentes, incluidas comunicaciones con contenido promocional, sobre servicios propios de PECB que sean similares o estén estrechamente relacionados con dicha relación y que se consideren razonablemente pertinentes o importantes. Dichas comunicaciones pueden enviarse sobre la base de los intereses legítimos de PECB o de una excepción aplicable relativa a clientes existentes, y los destinatarios pueden oponerse o darse de baja en cualquier momento.

PECB puede enviar comunicaciones de servicio no promocionales necesarias para:

- Crear o gestionar cuentas;
- Administrar certificaciones, capacitaciones, exámenes, solicitudes, pagos o facturas;
- Proporcionar atención al cliente;
- Comunicar asuntos de seguridad, legales, regulatorios, de acreditación, de políticas o contractuales; o
- Notificar a los usuarios los cambios que afecten a los servicios activos.

Por lo general, los destinatarios no pueden optar por dejar de recibir las comunicaciones de servicio necesarias mientras la cuenta, inscripción, certificación, examen, contrato o servicio correspondiente permanezca activo. Las comunicaciones de servicio no deben incluir contenido promocional innecesario.

Los socios independientes de PECB pueden procesar Datos Personales y enviar comunicaciones de acuerdo con sus propias declaraciones de privacidad. PECB no es responsable de las actividades de marketing independientes de un socio.

14. Conservación y Eliminación Segura

Los Datos Personales deben conservarse de acuerdo con el calendario de conservación aprobado de PECB.

Los periodos de conservación deben tener en cuenta:

- La finalidad original del procesamiento;
- Las obligaciones contractuales;
- Los requisitos de certificación, acreditación, exámenes y capacitación;
- Las obligaciones legales, regulatorias, financieras y contables;
- Los plazos relativos a reclamaciones, apelaciones, prescripción, auditorías e investigaciones;
- Los requisitos de prevención del fraude; y
- Las necesidades probatorias legítimas.

PECB debe revisar periódicamente los Datos Personales conservados.

Cuando la información ya no sea necesaria, debe eliminarse o destruirse de forma segura, anonimizarse de manera irreversible o eliminarse de otro modo mediante un método aprobado.

Los registros en formato impreso deben triturarse de forma segura o destruirse mediante un servicio aprobado de destrucción confidencial. Los registros electrónicos deben eliminarse utilizando métodos aprobados que sean adecuados para el sistema y el medio de almacenamiento.

Cuando la eliminación inmediata de las copias de seguridad no sea técnicamente viable, se debe restringir el acceso y la información no debe restaurarse ni utilizarse, salvo para fines legítimos de recuperación.

La eliminación puede suspenderse cuando la información esté sujeta a una obligación de conservación por motivos legales, una investigación, una reclamación, una apelación, una auditoría, un requisito regulatorio o de acreditación, o una reclamación legal existente o prevista.

15. Seguridad de los Datos y Prácticas de Trabajo

PECB debe implementar medidas técnicas, físicas y organizativas proporcionales a la naturaleza, el volumen, la sensibilidad, el contexto y el riesgo de los Datos Personales procesados.

Los controles pueden incluir:

- La clasificación de la información, el principio de privilegio mínimo, el acceso basado en la necesidad de conocer y la segregación de funciones;
- La autenticación robusta, la autenticación multifactor y las revisiones periódicas de los accesos;
- El cifrado en tránsito y en reposo, cuando corresponda;
- Los protocolos de comunicación seguros, el registro de eventos, el seguimiento y la prevención de pérdida de datos;
- Los controles de dispositivos terminales, cortafuegos, redes, vulnerabilidades y gestión de parches;
- Los controles de copias de seguridad seguras, recuperación, continuidad del negocio y recuperación ante desastres;
- Los controles de acceso físico y las prácticas de escritorio limpio;
- Las prácticas de desarrollo seguro de software, las pruebas de penetración y las evaluaciones de seguridad; y
- Los mecanismos aprobados de conservación y eliminación segura.

15.1. Registros Electrónicos y Físicos

Los Datos Personales electrónicos deben almacenarse y transmitirse únicamente mediante sistemas, dispositivos, servicios en la nube y métodos seguros aprobados. No deben conservarse copias locales innecesarias en dispositivos personales o no aprobados.

Los registros físicos deben almacenarse en áreas cerradas con llave o protegidas de otro modo, ser accesibles únicamente para el personal autorizado, estar protegidos durante su transporte y destruirse de forma segura cuando ya no sean necesarios.

15.2. Medios Extraíbles

Los Datos Personales no deben almacenarse en medios extraíbles sin una necesidad empresarial documentada y la autorización correspondiente. Los medios extraíbles aprobados deben cifrarse cuando sea viable, protegerse físicamente, someterse a seguimiento cuando corresponda y borrarse de forma segura o destruirse después de su uso.

15.3. Prácticas del Personal

El personal debe:

- Bloquear las pantallas cuando los dispositivos estén desatendidos;
- Proteger las contraseñas y las credenciales de autenticación;
- Verificar a los destinatarios antes de transmitir Datos Personales;
- Evitar los canales de comunicación o almacenamiento no aprobados;
- Utilizar únicamente aplicaciones y ubicaciones de almacenamiento autorizadas;
- Impedir que personas no autorizadas puedan ver información o escuchar conversaciones; y
- Informe inmediatamente de cualquier actividad sospechosa.

16. Encargados del Tratamiento, Proveedores de Servicios y Socios

Antes de designar a un encargado del tratamiento, intermediario de datos, proveedor de servicios en la nube, proveedor de software u otro proveedor de servicios que vaya a procesar Datos Personales, PECB debe llevar a cabo una debida diligencia proporcional en materia de privacidad y seguridad.

La debida diligencia debe tener en cuenta:

- La naturaleza, la sensibilidad, la finalidad y el volumen del procesamiento;
- Las ubicaciones del procesamiento y almacenamiento;
- Los controles de seguridad y el historial de violaciones;
- El apoyo para atender las solicitudes de los Titulares de los Datos; y
- Los acuerdos relativos a las transferencias internacionales.

Los acuerdos por escrito deben abordar, cuando corresponda:

- El objeto, la duración, la naturaleza y la finalidad del procesamiento;
- Las instrucciones documentadas y la confidencialidad;
- Los requisitos de seguridad;
- La asistencia para atender las solicitudes de los Titulares de los Datos y responder ante violaciones;
- Los derechos de auditoría y aseguramiento;
- Las transferencias internacionales;
- La devolución o eliminación de los Datos Personales; y
- Las obligaciones en caso de terminación.

Los encargados del tratamiento y los intermediarios de datos procesan los datos de acuerdo con sus propias políticas de privacidad.

Cuando PECB actúe como encargado del tratamiento o intermediario de datos, debe cumplir el contrato correspondiente, las instrucciones documentadas y la legislación aplicable.

Los socios independientes son responsables de las actividades de procesamiento para las que determinan los fines y los medios. Cuando PECB y otra organización determinen conjuntamente dichos fines y los medios esenciales, sus responsabilidades deben documentarse mediante un acuerdo adecuado.

17. Transferencias Internacionales de Datos

Los Datos Personales deben transferirse fuera de Singapur, del EEE o de otra jurisdicción de origen únicamente de conformidad con la legislación aplicable.

Para las transferencias desde Singapur, PECB debe adoptar las medidas adecuadas para garantizar que el destinatario en el extranjero proporcione un nivel de protección comparable al exigido por la PDPA de Singapur y el RGPD.

Las garantías permitidas pueden incluir:

- Las obligaciones contractuales;
- Normas corporativas vinculantes o acuerdos internos del grupo;
- Certificaciones reconocidas legalmente;
- Exenciones legales;
- Otros mecanismos permitidos por la ley.
- Una decisión de adecuación;
- Cláusulas Contractuales Estándar;

18. Divulgación de Datos Personales

PECB puede divulgar Datos Personales únicamente:

- Para una finalidad autorizada y documentada;
- Con un consentimiento válido cuando sea necesario;
- A un encargado del tratamiento, proveedor de servicios o socio autorizado de PECB que haya sido aprobado;
- A organismos de acreditación o certificación cuando sea necesario;
- A las autoridades competentes;
- Cuando lo exijan la ley, una orden judicial o un proceso legal;
- Para la formulación, el ejercicio o la defensa de reclamaciones legales;
- Para proteger los derechos, la propiedad, la integridad física o la seguridad de PECB o de terceros; o
- Cuando exista otra autorización legal aplicable.

Las solicitudes de tribunales, organismos reguladores, organismos encargados del cumplimiento de la ley o autoridades públicas deben revisarse para verificar su licitud, alcance y autenticidad. Se debe obtener asesoramiento jurídico cuando corresponda.

Solo deben divulgarse los Datos Personales mínimos que sean legal o razonablemente necesarios.

19. Gestión de Violaciones de Datos Personales

Todas las sospechas o confirmaciones de Violaciones de Datos Personales deben notificarse inmediatamente a través del proceso de notificación de incidentes de PECB. El personal no debe retrasar la notificación mientras intenta investigar de forma independiente.

PECB debe:

- Contener el incidente y preservar las pruebas pertinentes;
- Identificar los sistemas, registros, categorías de datos, volumen aproximado y personas afectados;
- Evaluar la causa, el impacto, la probabilidad y la gravedad del daño;
- Determinar los requisitos y plazos de notificación aplicables;
- Notificar a las autoridades competentes y a las personas afectadas cuando sea necesario;
- Documentar la evaluación, las decisiones y las notificaciones;
- Implementar acciones correctivas y preventivas; y
- Revisar la eficacia de la respuesta.

Todas las violaciones deben registrarse, incluidas aquellas que no requieran notificación externa.

Cuando sea aplicable la PDPA de Singapur, PECB debe evaluar si se requiere notificar a la Comisión de Protección de Datos Personales y a las personas afectadas dentro de los plazos establecidos.

Cuando sea aplicable el RGPD, PECB debe evaluar si se requiere notificar a la autoridad de control competente y comunicar la violación a los Titulares de los Datos afectados.

Los encargados del tratamiento, los intermediarios de datos, los proveedores de servicios y los socios deben estar obligados contractualmente a notificar a PECB las violaciones pertinentes sin dilación indebida.

Los empleados y contratistas no deben notificar de forma independiente a las personas afectadas, las autoridades, los clientes, los socios o los medios de comunicación, salvo que estén autorizados. El Responsable de Protección de Datos debe encargarse de gestionar la violación correspondiente y de comunicarse con las partes interesadas pertinentes al respecto.

19.1. Capacitación, Seguimiento y Cumplimiento

El personal con acceso a Datos Personales debe recibir capacitación adecuada en materia de privacidad y seguridad de la información:

- Al incorporarse a PECB;
- Periódicamente a partir de entonces;
- Cuando sus responsabilidades cambien sustancialmente; y
- Tras cambios significativos en la legislación, las políticas, los sistemas o los riesgos.

Se debe proporcionar capacitación específica según la función, cuando corresponda, al personal que participe en la gestión de solicitudes de los Titulares de los Datos, marketing, recursos humanos, tecnología de la información, seguridad de la información, exámenes, certificación, gestión de socios, respuesta a incidentes o procesamiento de alto riesgo.

PECB debe evaluar el cumplimiento mediante actividades proporcionales de:

- Revisión de la privacidad y los riesgos;
- Auditorías internas;
- Pruebas de seguridad;
- Seguimiento de las acciones correctivas.

Las no conformidades, debilidades y violaciones deben documentarse y abordarse. Los asuntos importantes deben notificarse al Responsable de Protección de Datos y a la Alta Dirección.

El incumplimiento puede dar lugar a medidas disciplinarias, restricciones de acceso, medidas contractuales, terminación de la relación laboral o contractual, acciones legales o notificaciones a las autoridades regulatorias cuando sea necesario.

20. Excepciones a la Política

Una excepción a esta Política puede aprobarse únicamente cuando:

- Exista una necesidad empresarial, legal, regulatoria o técnica documentada;
- Se hayan evaluado los riesgos para la privacidad y la seguridad;
- Se implementen medidas de protección alternativas adecuadas;
- El Responsable de Protección de Datos apruebe la excepción;
- La excepción tenga un alcance y una duración limitados; y
- La excepción se revise periódicamente.

Ninguna excepción puede autorizar un procesamiento ilícito.

21. Revisión de la Política

Esta Política debe revisarse al menos una vez al año y cuando se produzca:

- Un cambio significativo en la legislación aplicable;
- Un cambio significativo en la estructura, las ubicaciones operativas, los sistemas, los servicios o las actividades de procesamiento de PECB;
- Una Violación de Datos Personales significativa;
- Un hallazgo regulatorio, de acreditación o de auditoría;
- Un cambio significativo en los riesgos para la privacidad o en las responsabilidades de la organización.

El Responsable de Protección de Datos debe coordinar la revisión.

22. Contacto y Notificación

Las preguntas, inquietudes, solicitudes de los Titulares de los Datos, sospechas de Violaciones de Datos Personales o posibles incumplimientos de la Política deben notificarse a:

Responsable de Protección de Datos
Correo electrónico: dpo@pecb.com

Especialista en Operaciones de Seguridad de la Información
Correo electrónico: information.security@pecb.com

Centro de Ayuda del Servicio de Atención al Cliente de PECB

Correo electrónico: support@pecb.com

Los Titulares de los Datos del EEE también pueden ponerse en contacto con el Representante en el EEE ubicado en Lisboa, Portugal.

Representante en el EEE
Correo electrónico: gdpr.representative@pecb.com