Política de privacidad y conservación de datos biométricos para el registro de tiempo

Registro voluntario de tiempo mediante escaneo del dedo en PLA y sus empresas operativas

ID de política: HR-45-N2	**Revisión de biblioteca: 2.0**
Responsable: Recursos Humanos	**Idioma: Español**
Fecha de revisión: 16 de noviembre de 2026	**Vigencia: A partir de su publicación pública y su entrega a los trabajadores afectados**
Estado: Aprobado	**Continuidad: Se mantienen los derechos existentes** **Sustituye a HR-45-N2 y HR-45-F1, revisión de biblioteca 1.0 (24 de octubre de 2026).**

1. Propósito y alcance

PLA y sus empresas operativas (la Compañía) protegen los identificadores y la información biométricos utilizados para identificar a una persona. Una plantilla matemática derivada del escaneo de un dedo es información biométrica protegida, aunque no se conserve una imagen de la huella dactilar. Esta política cubre a toda persona cuya información biométrica la Compañía recopile o controle, incluidos los trabajadores de agencias de empleo y los contratistas; no autoriza la inscripción de ninguna persona ni grupo adicional.

El programa autorizado se limita a la verificación voluntaria de identidad mediante escaneo del dedo para registrar el tiempo con exactitud a través del sistema de registro de tiempo de ADP aprobado y sus proveedores identificados. El programa autorizado no debe conservar imágenes de huellas dactilares. RH y el responsable del sistema deben verificar el procesamiento real de los escaneos y la eliminación de datos del lector e informar sobre ello antes de la inscripción. El reconocimiento facial, las huellas de voz, los escaneos de iris o retina, otros sistemas biométricos y los nuevos propósitos requieren revisión y autorización por separado antes de la recopilación. Las funciones ordinarias de gafete, PIN, reloj web o geocerca no demuestran que se recopile información biométrica.

2. Cómo y dónde funciona el programa

En un centro de trabajo aprobado, el lector mide puntos del dedo durante la inscripción y crea una plantilla matemática. Un escaneo posterior se compara con esa plantilla para verificar la identidad de quien registra una entrada de tiempo. El lector específico, el modo de comparación, el almacenamiento de las plantillas, las transferencias y los destinatarios deben verificarse para ese centro y describirse en el aviso antes de la inscripción. Trate las plantillas almacenadas en los relojes, en los sistemas centrales y por los proveedores de servicios como información protegida.

RH y el responsable del sistema de registro de tiempo deben mantener un registro actualizado de centros de trabajo y dispositivos que indique la dirección física de trabajo, el empleador legal, el modelo y la función habilitada, los datos recopilados, las ubicaciones de almacenamiento, los proveedores, la versión del consentimiento, la alternativa disponible y el proceso de eliminación. Un pedido de equipo, una instrucción de inscripción o la disponibilidad de una función de ADP no bastan para demostrar su uso actual. No habilite un centro ni modifique sustancialmente su programa hasta confirmar estos controles y los requisitos estatales y locales aplicables.

3. Elección voluntaria y pago correcto

Proporcionar información biométrica no es un requisito para obtener ni conservar el empleo. Una persona puede negarse sin consecuencias laborales adversas o revocar su consentimiento en cualquier momento notificando a RH o a su gerente, presentando una solicitud escrita o utilizando el mismo método electrónico ofrecido para consentir u otro de sencillez similar.

Revocar el consentimiento debe ser tan fácil como otorgarlo. Los gerentes deben organizar con prontitud la alternativa tradicional de tarjeta de tiempo en papel y no deben presionar a una persona para que se inscriba, escanee otros dedos o vuelva a intentarlo después de negarse o revocar el consentimiento. Solo podrá ofrecerse otra opción no biométrica después de verificarla y comunicarla; la opción en papel seguirá disponible.

Registre y pague todo el tiempo remunerable, incluso cuando falle un lector, la inscripción esté incompleta, el sistema esté desconectado o se haya rechazado el consentimiento. No retrase una entrada de tiempo ni el pago de salarios por un problema biométrico. No cobre al trabajador por una inscripción solicitada por el empleador.

4. Aviso y consentimiento informado antes de la recopilación

Antes de recopilar u obtener información biométrica, proporcione un aviso escrito completo y comprensible que identifique al empleador real, el centro de trabajo, la información recopilada, el propósito específico, el almacenamiento y uso, el plazo de conservación, los destinatarios y los derechos aplicables. Entregue a la persona esta política y cualquier aviso de privacidad aplicable. Complete HR-45-F1 con los datos reales del programa y obtenga el consentimiento informado por escrito o un consentimiento electrónico legalmente válido antes de la inscripción. Obtenga cualquier permiso adicional exigido para la divulgación y renueve el consentimiento antes de un uso nuevo sustancial.

Utilice la función aplicable de aviso y consentimiento de ADP, además del aviso y consentimiento de la Compañía que cumplan los requisitos legales. Vincule la decisión tomada en el dispositivo con la versión del aviso, su entrega y la elección real. Un acuse general del manual, un formulario en blanco o un botón ACCEPT sin explicación no son suficientes. Si falta el consentimiento requerido, o este se rechaza o revoca, no recopile información biométrica ni continúe su uso. Aplique la alternativa. Ponga esta política de conservación y destrucción a disposición del público donde sea obligatorio, incluido Illinois; una carpeta restringida de Teams o de RH por sí sola no satisface ese requisito.

Inscripciones existentes. Para cada persona inscrita antes de la emisión de esta revisión, RH debe confirmar, dentro de los 60 días posteriores a la emisión, que consten en archivo un aviso completado y un consentimiento firmado o un consentimiento electrónico legalmente válido que cubran el programa real. En Illinois y Colorado, suspenda de inmediato el uso biométrico para la persona hasta que se haga esa confirmación. En los demás lugares, si la confirmación no se hace dentro de los 60 días, ofrezca HR-45-F1 y suspenda el uso biométrico hasta que la persona otorgue su consentimiento. Si la persona se niega o no responde, utilice la tarjeta de tiempo en papel y elimine la plantilla conforme a la sección 7. No solicite un nuevo consentimiento cuando ya conste en archivo una prueba válida y vigente. Un nuevo consentimiento no subsana una recopilación anterior; el departamento Legal decide cualquier medida correctiva para períodos anteriores.

5. Uso limitado, divulgación y protección

Utilice la información biométrica únicamente para el propósito informado de identidad y registro de tiempo. No la venda, arriende, intercambie ni obtenga ganancias de ella de otro modo, no la utilice para publicidad o entrenamiento de modelos ni la divulgue para un propósito ajeno. Limite el acceso al personal autorizado y a los proveedores de servicios identificados que tengan una necesidad lícita. Los contratos deben abordar los límites del propósito, la confidencialidad, las medidas de protección, los subencargados del tratamiento, los incidentes y la eliminación permanente oportuna. Un contrato por sí solo no autoriza una divulgación.

Divulgue o vuelva a divulgar información únicamente conforme a un fundamento permitido por la ley biométrica aplicable y después de obtener el consentimiento requerido. En Texas, el artículo 503.001(c) del Código de Negocios y Comercio permite la divulgación únicamente por los fundamentos que enumera, y el consentimiento por sí solo no es uno de ellos. La posición de la Compañía es que ADP y los demás proveedores identificados almacenan y procesan las plantillas únicamente como proveedores de servicios de la Compañía, conforme a un contrato escrito, para el propio propósito de registro de tiempo de la Compañía, y no las reciben para su propio uso. El departamento Legal debe documentar esa posición y las condiciones contractuales que la respaldan. No proporcione información biométrica de Texas a ninguna otra persona, salvo que el departamento Legal confirme un fundamento enumerado en el artículo 503.001(c). Utilice, como mínimo, el cuidado razonable del sector y medidas al menos tan protectoras como las utilizadas para otra información confidencial y sensible. Exija cifrado, controles de acceso y transmisión segura apropiados, verifique las configuraciones reales y no envíe plantillas biométricas por correo electrónico ni las coloque en expedientes de personal o carpetas generales de Teams.

6. Conservación y destrucción permanente

Conserve la información biométrica únicamente mientras continúe el propósito informado. Destrúyala permanentemente sin demora cuando se cumpla el propósito, incluido el fin del empleo o de la asignación correspondiente, el traslado a un trabajo sin uso biométrico, la suspensión definitiva del programa o una revocación efectiva que ponga fin al propósito. Destrúyala a

más tardar tres años después de la última interacción de la persona con la Compañía, o antes si lo exige la ley aplicable. Para la información recopilada en Illinois, la única excepción a estos plazos es una orden de registro o una citación judicial válida emitida por un tribunal competente. En los demás lugares, solo se aplica una excepción cuando el departamento Legal confirma por escrito la ley u orden judicial específica que exige una conservación más prolongada y la fecha en que termina ese requisito. No aplique a las plantillas biométricas un plazo general de conservación de expedientes de personal.

Para Colorado, aplique también los supuestos legales de destrucción anticipada y la revisión anual indicados a continuación. El fin del propósito autorizado sigue siendo la regla de la Compañía que exige la destrucción antes. Conserve únicamente las pruebas separadas, mínimas y lícitas del aviso, consentimiento, revocación y destrucción completada conforme al calendario de conservación de registros aplicable; no conserve el identificador biométrico como prueba de cumplimiento.

7. Eliminación por ADP y otros custodios

RH debe notificar con prontitud al responsable del sistema cuando ocurra un supuesto de destrucción. El responsable debe detener el uso biométrico, organizar la alternativa si es necesaria, solicitar la eliminación permanente a ADP y a todos los proveedores correspondientes, eliminar las plantillas de cada reloj y sistema central pertinente y verificar que se haya completado. Documente el supuesto que originó la eliminación, la solicitud, los sistemas afectados y la confirmación sin conservar la plantilla.

No suponga que una baja en RH, un gafete deshabilitado, la eliminación del acceso a una aplicación o un estado de consentimiento Accepted demuestran que se haya eliminado la plantilla. Verifique el funcionamiento real de la eliminación automática y manual del producto, la sincronización de dispositivos y las copias de respaldo. Los términos de conservación de ADP para el registro de tiempo no sustituyen los plazos legales o de política más cortos de la Compañía. Si una obligación alegada de preservación entra en conflicto con la destrucción, RH o Legal deben determinar la excepción y el plazo legales exactos. En Illinois, solo una orden de registro o una citación judicial válida emitida por un tribunal competente retrasa la destrucción. Una orden general de preservación no permite la conservación indefinida de datos biométricos.

8. Requisitos estatales y locales

Determine la ley aplicable según los lugares reales de trabajo y recopilación y otros vínculos jurídicamente pertinentes, incluidos la residencia y el lugar donde se procesa o divulga la información. Incluya el trabajo remoto y las normas municipales aplicables. Illinois exige una política pública de conservación y un consentimiento informado por escrito antes de la recopilación, con destrucción cuando se cumpla el propósito inicial o dentro de los tres años posteriores a la última interacción, lo que ocurra primero. Su disposición sobre firmas electrónicas no elimina las obligaciones de aviso ni de consentimiento.

Colorado exige una política escrita, un procedimiento de respuesta a incidentes, una revisión anual de necesidad, aviso previo y consentimiento para la recopilación de datos biométricos de empleados sujeta a la ley. Su plazo de destrucción es la fecha que ocurra primero entre el cumplimiento del propósito, 24 meses después de la última interacción de la persona o la fecha más próxima razonablemente factible dentro de los 45 días posteriores a una revisión anual o más frecuente que determine que la conservación ya no es necesaria, adecuada o pertinente para el propósito informado. Una prórroga específica permitida por ley para ese plazo basado en la revisión no amplía un plazo anterior por fin del propósito o última interacción. Informe la categoría real de datos, el propósito, el plazo de conservación y las divulgaciones; aplique las reglas adicionales de consentimiento para la divulgación y las restricciones sobre los propósitos de uso en el empleo. La elección voluntaria de la Compañía se aplica incluso cuando una disposición legal limitada permitiría imponer un requisito.

Texas exige aviso y consentimiento antes de la captura con fines comerciales y, por regla general, exige la destrucción dentro de un plazo razonable, a más tardar un año después de que expire el propósito, sujeto a sus excepciones específicas. Se aplica nuestra regla de destrucción al finalizar el propósito, que exige hacerlo antes. Nueva York prohíbe exigir las huellas dactilares de un empleado como condición para obtener o conservar el empleo, salvo lo dispuesto por ley. California restringe la entrega a terceros de huellas dactilares de empleados que pudiera perjudicarlos y, cuando se aplica la CCPA, exige un aviso al momento de la recopilación y los derechos de privacidad correspondientes. Aplique el alcance y las excepciones específicos de la ley de Washington en lugar de suponer una exención general para empleados. El consentimiento nunca subsana un uso prohibido.

9. Incidentes, preguntas y derechos protegidos

Informe con prontitud cualquier sospecha de pérdida, acceso no autorizado o divulgación a RH y por el canal de TI o seguridad correspondiente. El personal autorizado de respuesta debe contener el incidente, evaluar su alcance e impacto y coordinar los avisos exigidos. Notifique a las personas afectadas y a las autoridades según lo exigido, sin demora injustificada y a más tardar 30 días después del descubrimiento, aplicando cualquier plazo legal más corto y únicamente una demora específicamente permitida. Elimine permanentemente los identificadores comprometidos de los sistemas afectados, salvo que exista una

obligación específica de conservación lícita; RH o Legal deben conciliar esa obligación con la destrucción obligatoria y documentar la decisión.

Comuníquese con RH o su gerente para obtener el aviso vigente, una copia de la política, la opción de tarjeta de tiempo en papel o ayuda para revocar el consentimiento o presentar una solicitud de privacidad. Report It y otras vías protegidas de denuncia siguen disponibles. La Compañía prohíbe las represalias por negarse, revocar el consentimiento o ejercer un derecho protegido. Esta política no supone una renuncia a derechos legales ni modifica un acuerdo separado ya firmado. Aplique HR-18, HR-45 y HR-46 conjuntamente con esta política y la legislación vigente aplicable.