Cómo la aplicación del GDPR de Blackboard respalda a nuestros clientes

El Reglamento general de protección de datos (GDPR, por sus siglas en inglés) de la UE es un cambio radical. Blackboard ve con buenos ojos este cambio. Nos importa la privacidad de los datos y entendemos que es un derecho humano. El GDPR fortalece los derechos de los individuos y llevará a mejores prácticas de privacidad de datos. Esto beneficiará a los individuos y a las organizaciones ya que aumentará la confianza entre ellos.

Publicamos este documento para brindarles a nuestros clientes un resumen de los cambios y los mitos en torno al GDPR, para explicar nuestro enfoque de aplicación y para detallar cómo nuestros esfuerzos respaldarán a su organización. Nos enfocamos en la información que creemos que les será más útil. Por lo tanto, este libro blanco no es de ninguna manera una guía exhaustiva del GDPR.[1]

El GDPR trae consigo cambios significativos, pero en Blackboard se puede construir sobre la base de nuestras sólidas prácticas de privacidad de datos ya existentes (por ejemplo, nuestra certificación del Escudo de privacidad UE-EUA). Consideramos que el GDPR es una oportunidad para fortalecer aún más nuestras prácticas. Nuestro enfoque seguirá orientado al cliente y lo respaldaremos en su cumplimiento de la privacidad de datos.

Estos materiales han sido preparados únicamente con fines informativos y no constituyen asesoramiento jurídico. Sírvase solicitar asesoramiento de sus abogados internos o externos para la aplicación del GDPR en su organización y cuestiones jurídicas relacionadas.

CONTENDIO

GDPR – LO QUE TIENE QUE SABER

Blackboard cuenta con la certificación del Escudo de privacidad, es orgulloso signatario del Compromiso de privacidad del estudiante y miembro del Foro del futuro de la privacidad.

El GDPR es la nueva legislación sobre protección de datos de la UE que reemplazará la actual Directiva de protección de datos de la UE 96/46 (Directiva) y las Leyes de protección de datos aplicables en los Estados miembros de la UE (por ejemplo, la Ley de protección de datos de Reino Unido de 1998).

El GDPR se promulgó en mayo de 2016 con fecha de cumplimiento el 25 de mayo de 2018.

En las secciones de siguen a continuación, se ha provisto un resumen muy breve (que dista de ser exhaustivo) sobre los requisitos del GDPR. Los enlaces a pautas más detalladas se pueden encontrar en la sección «Recursos útiles del GDPR».

¿Por qué una ley nueva?

Los legisladores y reguladores en la UE estaban convencidos de que la Directiva necesitaba una actualización que abordara la falta de armonización y los desarrollos sociales y tecnológicos de los 20 años posteriores a la Directiva. Facultades coercitivas más fuertes, alcance territorial más amplio y afianzamiento de derechos para individuos encabezaban la lista.

Muchas de las nuevas disposiciones (por ejemplo, efecto de extraterritorialidad) hacen referencia principalmente a empresas de redes sociales e internet fuera de la UE. Los legisladores y reguladores de la UE consideraban que la Directiva existente no protegía de manera suficiente los derechos de privacidad de datos de los individuos de la UE que usan dichos servicios de redes sociales e internet.

Blackboard opera de manera diferente a tales empresas de redes sociales y otras empresas de internet cuyo modelo se construye sobre la base de «monetizar» los datos del usuario. Recopilamos y usamos información personal[2] de nuestros clientes de acuerdo con sus indicaciones y con el fin de proveer nuestros productos y servicios a ellos y sus usuarios. No recopilamos ni usamos información personal para venderla ni para vender publicidad. Entendemos que se nos confía información personal y que esto conlleva responsabilidades. Por lo tanto, tenemos una responsabilidad y un interés compartidos con nuestros clientes en la salvaguarda de esta información.

¿Qué es lo nuevo?

Si bien se basa en principios y conceptos de privacidad de datos de la UE existentes, el GDPR trae consigo cambios significativos al régimen de privacidad de datos en la UE, los que incluyen:

- Mayores facultades sancionatorias de hasta 4 % del volumen global o 20 millones de euros (el monto que sea mayor)
- Alcance territorial más amplio para organizaciones fuera de la UE que proveen productos y servicios a residentes de la UE o que monitorean a los residentes de la UE
- Notificación de filtración obligatoria a autoridades supervisoras en 72 horas para los controladores de datos[3]
- Requisitos más estrictos respecto al consentimiento
- Afianzamiento de derechos de los individuos (los que incluyen el derecho a la supresión y portabilidad de datos)

Pero algunos de los cambios más importantes son los nuevos principios de responsabilidad y privacidad por diseño. Estos principios requieren procesos y gobernanza eficaces respecto a la privacidad de datos así como también documentación más detallada y sólida sobre cómo una organización cumple con los requisitos del GDPR.

¿Qué no cambia?

Muchos de los conceptos y definiciones en el GDPR permanecen iguales o son similares en comparación con la Directiva:

- La definición de «datos personales» (o información personal) permanece igual en líneas generales, pero ahora incluye expresamente direcciones IP, cookies e identificadores del dispositivo.
- Los conceptos de «controlador de datos» y «procesador de datos» permanecen iguales (pero el GDPR impone responsabilidades más directas a los procesadores de datos).[4]
- Se mantienen los principios para el procesamiento establecidos en la Directiva (por ejemplo, procesamiento legal y legítimo, limitación de fines, conservación de datos personales únicamente mientras sea necesario).
- Los requisitos para la transferencia de datos siguen siendo iguales en líneas generales: se permiten las transferencias de datos fuera de la UE o del EEE siempre que se use un mecanismo de transferencia de datos aprobado (por ejemplo, Escudo de privacidad UE-EUA o «cláusulas modelo»).[5]

El nivel más elevado de sanciones conforme al GDPR significa que es posible que el no cumplimiento con los principios y requisitos existentes, tal como conservar datos personales únicamente mientras sea necesario o tener medidas de seguridad adecuadas en funcionamiento, conlleve un mayor riesgo.

¿Cuál es el impacto del *brexit*?

El GDPR se aplicará directamente en Reino Unido a partir del 25 de mayo de 2018 hasta el «brexit», a fines de marzo de 2019. Pero, incluso luego del *brexit*, el GDPR fijará el estándar para el Reino Unido.

- El gobierno de Reino Unido ha publicado la Ley de protección de datos de Reino Unido de 2017 (actualmente en proceso legislativo) que aplica el GDPR antes y después del *brexit*[6]
- Luego del *brexit*, el GDPR aplica directamente a organizaciones del Reino Unido que ofrecen bienes y servicios a residentes de la UE o que los monitorean (por ejemplo, universidades del Reino Unido que reclutan estudiantes de la UE de forma activa).

Impacto en la transferencia de datos desde y hacia Reino Unido:

- La UE ha aclarado que, luego del *brexit*, Reino Unido será considerado un «tercer país», lo cual significa que ya no se considera un país «adecuado» (en la lista blanca) para la transferencia de datos.
- Salvo que la Comisión de la UE declare que Reino Unido es adecuado y hasta que esto suceda (por ejemplo, como parte de un acuerdo de transición), es necesario aplicar los acuerdos de transferencia de datos u otro mecanismo de transferencia de datos para la transferencia de información personal desde la UE hacia Reino Unido.
- Por el contrario, Reino Unido tiene que determinar qué países considera adecuados (los que probablemente incluirán países de la UE y países que la UE incluye en la lista blanca). En el caso de aquellos países que no se consideran adecuados, se tendrán que aplicar mecanismos de transferencia de datos reconocidos por Reino Unido (probablemente similares a los mecanismos de la UE) para las transferencias de información personal fuera de Reino Unido.

Desmitificación del GDPR

Un objetivo del GDPR era proveer más claridad mediante una propuesta más detallada. Sin embargo, todavía existen muchos aspectos del GDPR que se encuentran abiertos a interpretación. Además, la complejidad del GDPR ha llevado a una falta de comprensión, así como también declaraciones exageradas. Esto ha creado muchos mitos, algunos de los cuales desmentimos a continuación:[7]

Mito 1: Se requiere consentimiento para todo procesamiento de información personal

Hecho: El consentimiento es solo una de varias bases jurídicas que permiten que la información personal sea procesada (por ejemplo, procesamiento requerido para la ejecución de un contrato o para el «interés legítimo» de una organización). El umbral de consentimiento se ha vuelto muy alto. Por ejemplo, salvo que los individuos tengan una auténtica libertad de acción y puedan retirar su consentimiento en cualquier momento sin ninguna desventaja, no se considerará consentimiento válido. En muchos casos de procesamiento de datos serán más apropiadas otras bases jurídicas.[8]

Mito 2: El período de notificación de filtración de 72 horas aplica a la totalidad de la cadena de suministro (es decir, desde el momento en que un (sub)procesador tiene conocimiento de la filtración)

Hecho: El GDPR requiere que los procesadores de datos notifiquen a su controlador de datos «sin demora injustificada» en el caso de una filtración de datos personales. Solo una vez que el procesador de datos haya notificado al controlador es que comienza el período de notificación de 72 horas para el controlador de datos. En sus últimas pautas[9] , el Grupo de trabajo del artículo 29 (WP29, por sus siglas en inglés), el grupo de autoridades para la protección de datos de la UE, ha aclarado que «sin demora injustificada» significa una notificación «rápida» (no una notificación «inmediata», como se sugería en un borrador anterior).

Mito 3: No se permiten las transferencias de datos fuera de la UE o del EEE o solo con el consentimiento del cliente para cada transferencia de datos

Hecho: El GDPR mantiene en líneas generales los requisitos de transferencia de datos existentes. Como tales, se permiten las transferencias de datos si se aplica un mecanismo de transferencia de datos aprobado por la UE, tal como el Escudo de privacidad UE-EUA o las cláusulas modelo aprobadas por la UE (acuerdos sobre transferencia de datos). Blackboard aplica ambos mecanismos para transferir la información personal del cliente como es debido.[10] Dado que Blackboard actúa como un procesador de datos, se requiere una instrucción general para las transferencias de datos del cliente (lo cual está incluido en nuestro acuerdo de procesamiento de datos estándar), pero no es necesario el consentimiento del cliente para cada transferencia de datos.

Mito 4: El derecho de supresión requiere que las organizaciones supriman todos los datos de un individuo

Hecho: El nuevo derecho de supresión no es un «derecho a ser olvidado» absoluto. En cambio, es un derecho que se eliminen datos si estos ya no son requeridos y en otras circunstancias en las que la organización no cumple con los requisitos del GDPR. Si una organización todavía necesita conservar los datos de manera legítima (por ejemplo, debido a requisitos de conservación de registros), entonces esta información personal no tiene por qué suprimirse.

Mito 5: El GDPR aplica a todas las universidades que tienen estudiantes de la UE

Hecho: El simple hecho de contar con estudiantes de la UE inscritos no es suficiente para que aplique el GDPR. En general, el GDPR aplica a instituciones que están establecidas en la UE. También aplica a universidades fuera de la UE, pero solo si ofrecen bienes y servicios a individuos en la UE o si monitorean el comportamiento de los individuos en la UE. Para considerar que «ofrece servicios», se requiere un cierto grado de focalización. El mero hecho de tener inscritos estudiantes de la UE no es suficiente. Sin embargo, el GDPR puede aplicar cuando las universidades se focalizan activamente en residentes de la UE (por ejemplo, para cursos online) o reclutan estudiantes activamente en países de la UE. Estos criterios están abiertos a interpretación. Recomendamos que los clientes soliciten asesoramiento jurídico por su cuenta.

APLICACIÓN DEL GDPR

¿Por qué es importante entender la privacidad de datos y el GDPR?

El riesgo de multas de 4 % del volumen global es sin lugar a dudas la razón por la que muchas organizaciones han empezado a considerar más seriamente la privacidad de datos. Sin embargo, a nuestro entender, el caso a favor de las buenas prácticas de privacidad de datos es al menos igual de convincente ya que la privacidad de datos es un derecho humano y el hecho de contar con prácticas de privacidad de datos sólidas genera confianza.

En la sociedad de hoy en día, la información personal se encuentra en todos lados. Se suele hablar de la información personal como el nuevo petróleo de la economía. Todos usamos servicios en internet y cedemos nuestra información personal. Pero estudio tras estudio demuestran que no se confía en las organizaciones cuando de información personal se trata. La sensación es que los individuos han perdido el control de sus datos. Los legisladores y reguladores reaccionan a este hecho. Probablemente, el GDPR sea el ejemplo más notorio. Es necesario que las organizaciones vuelvan a ganarse la confianza de los individuos. Las buenas prácticas de privacidad de datos son la clave para construir esta confianza. Asimismo, son una ventaja competitiva. Por último, también ayudan a las organizaciones con la innovación. Si los estudiantes (y el personal) confían en su institución, será más probable que compartan su información y utilicen nuevas herramientas.

Las equivocaciones respecto a la privacidad de datos pueden ser catastróficas. En las noticias, con frecuencia se cubren filtraciones de datos. Lo que le sigue es un daño a la reputación, la pérdida de confianza de los individuos y el riesgo de demandas de aquellos cuyos datos han sido mal gestionados. Es posible que las autoridades para la protección de datos no utilicen las multas de 4 % del volumen global desde un principio, pero tienen a su disposición muchas otras herramientas para hacer cumplir la ley y pueden obligar a las instituciones a modificar sus prácticas de datos y poner en práctica programas sobre privacidad de datos con auditorías externas habituales.

El papel de nuestra organización y la suya conforme al GDPR

El GDPR mantiene el concepto de «controlador de datos» y «procesador de datos». Este concepto es clave ya que determina las responsabilidades y obligaciones y sus proveedores de servicios.

Se considera que una organización es un controlador de datos si determina los «medios y fines» del procesamiento de información personal, es decir, por qué y cómo se usa la información personal. Por otro lado, el procesador de datos es la organización que actúa en nombre del controlador de datos y conforme a sus instrucciones.

Respecto a la mayoría de los productos y servicios de Blackboard (por ejemplo, Learn, Collaborate, Open LMS), se considera que Blackboard es un procesador de datos y nuestros clientes son el controlador de datos.

El GDPR impone requisitos más directos sobre los procesadores de datos, tales como Blackboard. Sin embargo, la mayoría de los requisitos del GDPR aún aplican a los controladores de datos (por ejemplo, la responsabilidad de informar a los individuos cómo se usan sus datos, cumplir con las solicitudes de los individuos para acceder a sus datos, hacer llegar la notificación de filtración obligatoria a autoridades para la protección de datos e individuos).

¿Qué puede hacer para prepararse para el GDPR?

Todas las organizaciones que abarca el GDPR tendrán que estar preparadas el 25 de mayo de 2018. A continuación se presentan algunas cosas claves que los clientes pueden hacer para prepararse. Esta lista de etapas se basa en nuestra experiencia y de ningún modo pretende ser exhaustiva. Asegúrese de involucrar a expertos en la privacidad de datos para que ayuden en su aplicación. Muchas autoridades para la protección de datos también han creado sus pautas sobre cómo aplicar el GDPR.[11]

Con suerte, ya superó las etapas 1-6 y se encuentra en la mitad del camino para la aplicación de sus planes de acción. Pero nunca es demasiado tarde para empezar. Incluso si recién ha empezado, puede aplicar los cambios más importantes. También significa que será capaz de demostrar a su autoridad para la protección de datos que está trabajando en un plan. Ignorar el GDPR no es una opción.

1. Verificar que el GDPR se aplique a su organización

Si su organización se establece en la UE, entonces aplica el GDPR. Pero el GDPR también puede aplicar a organizaciones fuera de la UE.[12]

2. Establecer un proyecto del GDPR

Diseñar y aplicar un proyecto reservado al GDPR. De manera ideal, tendrá soporte de gestión de proyectos y contactos nominados que pueden dar apoyo en cada departamento. Este proyecto se extenderá a través de todos los departamentos de su institución y necesitará ayuda.

3. Nominar un líder de GDPR con experiencia para gestionar el proyecto

El líder no debe ser solo un líder de privacidad de datos con experiencia sino que también debe tener tiempo y recursos suficientes así como acceso a soporte externo (por ejemplo, estudio jurídico). Si su organización es una autoridad pública establecida en la UE también tendrá que designar un Director de protección de datos.

4. Garantizar participación y supervisión de altos directivos

La aplicación de un proyecto del GDPR es difícil sin el apoyo, las indicaciones y la supervisión de los altos directivos.

5. Revisar su uso de información personal y realizar análisis de deficiencias

La primera fase clave del proyecto del GDPR es comprender dónde y cómo se usa la información personal y en qué puntos se requiere el fortalecimiento del GDPR.

6. Desarrollar planes de acción para reducir deficiencias

Posiblemente esta sea la parte más difícil del GDPR ya que requiere convertir los requisitos que suelen ser de alto nivel del GDPR en acciones específicas y que se puedan poner en práctica en todos los procesos y sistemas.

7. Aplicar planes de acción

La confianza es algo positivo, pero en este caso es mejor el control. Esta fase requiere el seguimiento de los planes de acción de otros para asegurarse de que cumplan con sus plazos.

8. Evaluar a sus proveedores

De conformidad con el GDPR, ustedes son responsables de sus proveedores. Es importante contar con las disposiciones contractuales correctas, pero no es suficiente. Tienen que estar seguros de que los proveedores cumplen con los requisitos del GDPR y que pueden respaldarlos en su cumplimiento. Averigüen cómo están poniendo en práctica el GDPR.

9. Manténganse al día respecto a novedades legales o regulatorias (pautas del Grupo de trabajo del artículo 29, Estados miembros que aplican leyes)

Conocer el GDPR ya es suficiente, ¿no? ¡Error! Si bien el GDPR se aplica directamente, todos los Estados miembros de la UE están poniendo en práctica leyes de protección de datos complementarias a nivel nacional. Estas son necesarias para regular áreas en las que los Estados miembros tienen autoridad legislativa (por ejemplo, privacidad de datos de empleados) o en las que el GDPR hace posible que legislen adicionalmente (por ejemplo, criterios para las DPO [pruebas delegadas de estaca] y las DPIA [evaluaciones de impacto en la protección de datos]). De manera adicional, el WP29 publica pautas importantes. Mantenerse al día es un desafío pero importante.[13]

PLAN Y ENFOQUE DE BLACKBOARD

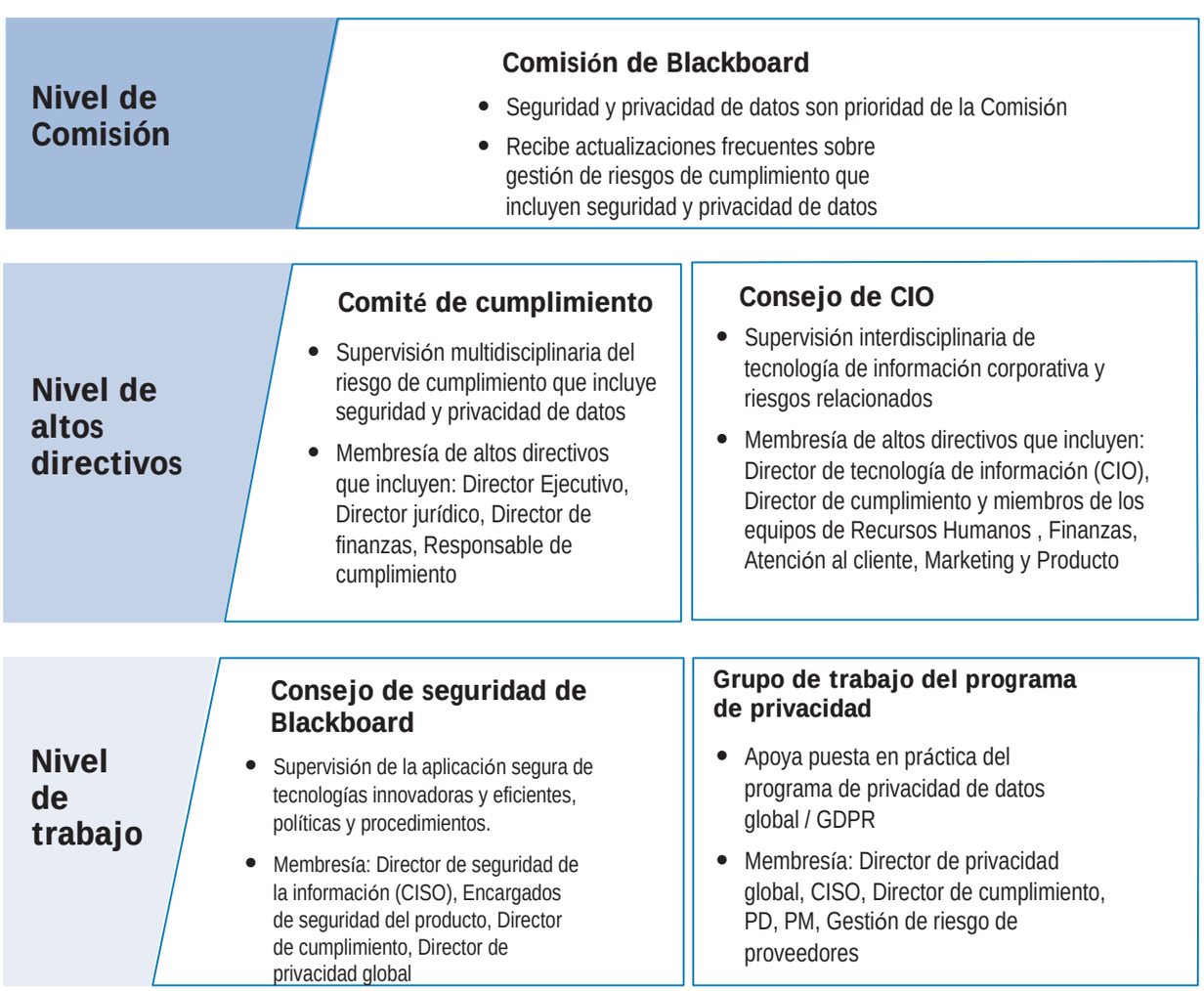
Seguridad y privacidad de datos en Blackboard

La seguridad y privacidad de datos ha sido una prioridad clave de larga data en Blackboard. A nuestro entender, el GDPR es una oportunidad para fortalecer aún más nuestras prácticas de privacidad de datos existentes.

Nuestro enfoque respecto a la privacidad de datos siempre ha sido orientado al cliente. Comprendemos los desafíos que enfrentan nuestros clientes y queremos ayudarlos junto con ustedes.

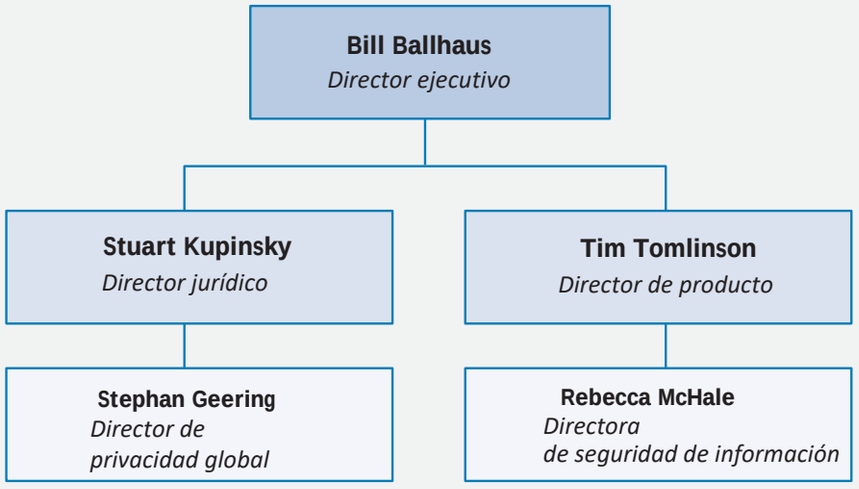
Las buenas prácticas de privacidad de datos requieren un modelo de gobernanza sólido. En Blackboard, la seguridad y privacidad de datos son una prioridad del Consejo y nuestro modelo de gobernanza (ver a continuación) asegura que los altos directivos supervisen y respalden nuestros esfuerzos para garantizar la seguridad y privacidad de datos.

La importancia que Blackboard le da a la seguridad y privacidad de datos también se destaca por el hecho de que nuestro Director de privacidad global y Director de seguridad de información[14] responden al Equipo de liderazgo del Director ejecutivo (ver gráfica organizacional a continuación).



Privacidad y seguridad

También se destaca la importancia que le da Blackboard a la seguridad y privacidad de datos por el hecho de que nuestro Director de privacidad global y Director Ejecutivo responden al Equipo de liderazgo del Director ejecutivo



Enfoque al GDPR de Blackboard

Se ha establecido un proyecto exhaustivo para cumplir con los requisitos del GDPR mediante el siguiente enfoque:

- La aplicación del GDPR se construye sobre la base de los mecanismos de cumplimiento y la experiencia de privacidad de datos existentes de Blackboard.
- El Director de privacidad global lleva a cabo la aplicación del GDPR y cuenta con el soporte de un gestor de proyectos dedicado y «líderes del GDPR» en cada área funcional.
- Se ha involucrado al reconocido estudio jurídico Bristows LLP, entre varios otros, para apoyar la aplicación del GDPR.
- El Comité de cumplimiento de Blackboard supervisa la aplicación del GDPR, el que incluye al Director Ejecutivo de la empresa, el Director jurídico y otros altos directivos.

GDPR como una oportunidad

Consideramos que la aplicación del GDPR no es un mero esfuerzo por cumplir con los nuevos requisitos de privacidad de datos de la UE, sino también una oportunidad. Como tal, nuestro objetivo es usar la aplicación del GDPR para lograr lo siguiente:

- Fortalecer las prácticas de privacidad de datos globales – haremos uso del proyecto del GDPR para fortalecer nuestro programa de privacidad de datos global en la UE y más allá.
- Desarrollar procesos de privacidad por diseño que incorporen el cumplimiento de privacidad de datos en nuestros procesos diarios.
- Apoyar a nuestros clientes en sus esfuerzos de cumplimiento del GDPR.
- Posicionar a Blackboard como el líder reconocido de privacidad de datos en Tecnología educativa.

Nuestro plan de aplicación

Estamos siguiendo la metodología establecida de tres fases de Bristow LLP para aplicar nuestro programa de privacidad de datos global / GDPR. Varias otras empresas, que incluyen empresas de tecnología de punta, están usando esta metodología. Las tres fases clave son las siguientes:

- **FASE 1 - Recopilación de información**
- **FASE 2 - Desarrollo de soluciones**
- **FASE 3 - Líneas de trabajo para la aplicación**

Se ha usado esta metodología de tres fases para desarrollar nuestro programa con las siguientes cuatro etapas claves:

Inicio del proyecto

La etapa de inicio del proyecto incluía las siguientes actividades:

- Sesión informativa y participación de altos directivos.
- Contratación de un Director de privacidad global con la responsabilidad de liderar el proyecto del GDPR
- Desarrollo del plan del proyecto y la gobernanza del proyecto.
- Recopilación inicial de información y evaluación de actividades de cumplimiento actuales para áreas que requieren fortalecimiento conforme al GDPR.

FASE 1 - Recopilación de información (talleres)

Durante esta fase inicial, llevamos a cabo talleres/conversaciones estructuradas con accionistas claves de las áreas funcionales y grupos de trabajo de Blackboard para obtener información detallada sobre prácticas de procesamiento de datos en dichas áreas.

El resultado de los talleres se usó para llevar a cabo el análisis deficiencias y desarrollar las soluciones y la puesta en práctica de los planes en la fase 2.

FASE 2 - Desarrollo de soluciones

Con base en la información de los talleres, desarrollamos las siguientes soluciones y documentación:

- Documentación sobre privacidad de datos internos mejorada (política y estándares operativos detallados) que refleja los requisitos del GDPR y explica cómo se tendrá que cumplir con los requisitos del GDPR para las distintas actividades de procesamiento de datos (por ejemplo, requisitos para el procesamiento de datos del cliente, el proceso de privacidad por diseño).
- Requisitos del producto
- Planes de aplicación para las áreas funcionales y para esfuerzos esencialmente requeridos.

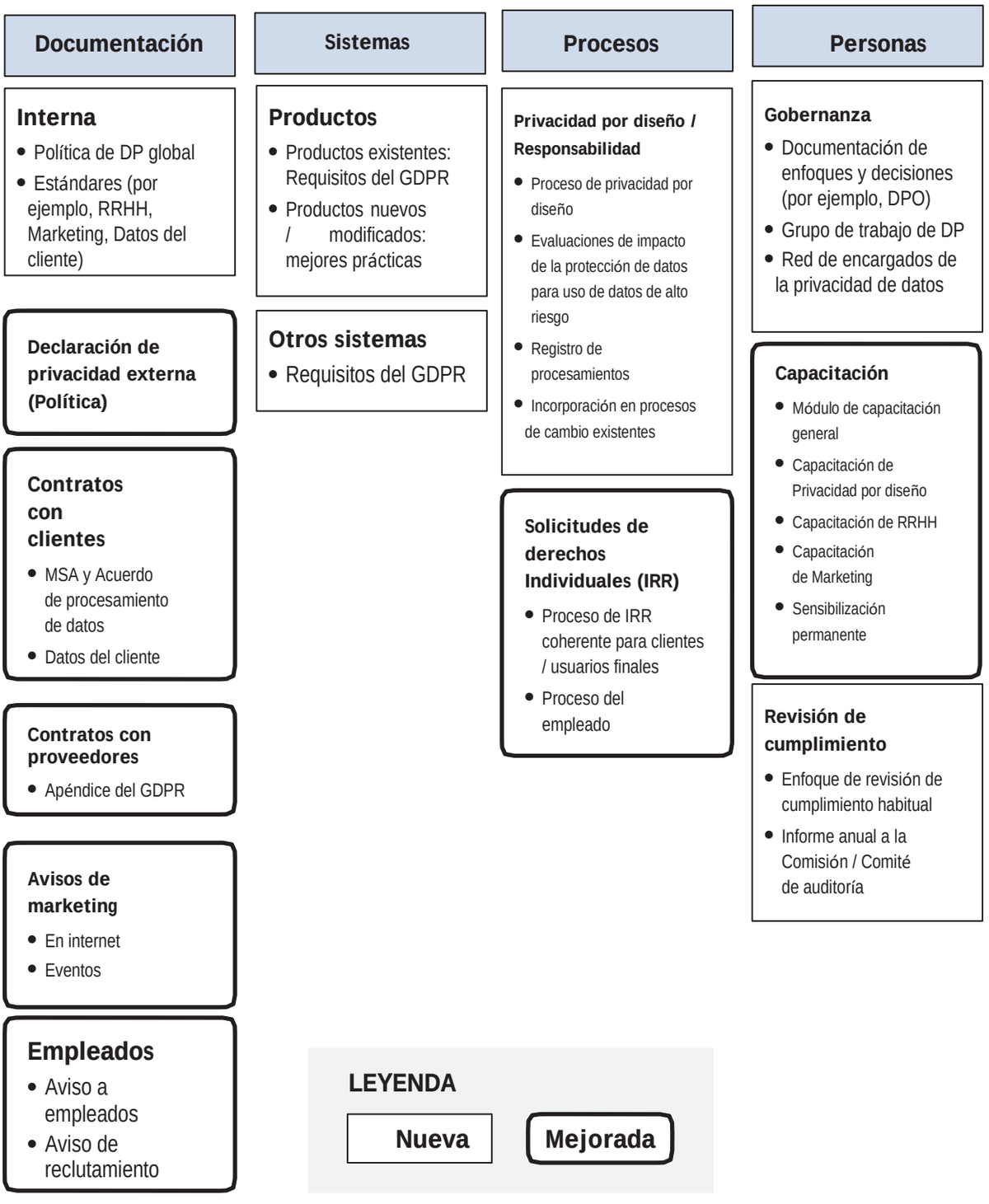
FASE 3 - Líneas de trabajo para la aplicación

Durante la fase final, se aplica la documentación de privacidad de datos desarrollada y se ejecutan los planes de aplicación. Se usarán seis líneas de trabajo principales para lograr la aplicación:

1. Ejecutar los planes de aplicación para las áreas funcionales y los grupos de producto.
2. Revisar y actualizar políticas, avisos y consentimientos orientados al público.
3. Fortalecer la gobernanza (roles y responsabilidades, capacitación, privacidad por diseño, etc.).
4. Revisar y actualizar los contratos del proveedor (en los casos que sea necesario).[15]
5. Cambios de sistemas informáticos (en los casos que sea necesario)
6. Establecer un registro de procesamiento de datos.

Resumen de cambios

La gráfica a continuación muestra cómo concebimos el estado final de nuestro programa de privacidad de datos / GDPR luego llevar a cabo las actividades. Luego de la aplicación del GDPR seguiremos con nuestra innovación y adaptación para el mayor crecimiento de las prácticas de privacidad de datos.



¿CÓMO LO AYUDARÁ NUESTRO PROGRAMA DEL GDPR?

El programa de aplicación de privacidad de datos globales / GDPR de Blackboard se enfoca en respaldar a su organización en la aplicación del GDPR. Las siguientes secciones proveerán más detalles pero, en resumen, los 7 puntos claves son:

1. **Productos preparados para el GDPR:** Estamos poniendo en práctica requisitos del producto para respaldar a los clientes con requisitos de transparencia, solicitudes de derechos individuales, etc.
2. **Privacidad por diseño:** Estamos poniendo en práctica un proceso de privacidad por diseño y evaluación del impacto de la protección de datos (DPIA) para facilitar la documentación de cumplimiento.
3. **Transferencias de datos:** Seguiremos con nuestro enfoque de múltiples capas: Regionalización, Escudo de privacidad UE-EUA y cláusulas modelo aprobadas por la UE.
4. **Contratos con clientes:** Tenemos un apéndice al acuerdo maestro estándar de procesamiento de datos preparado para el GDPR.
5. **Nuestros proveedores:** Contamos con contratos sólidos y un marco de gestión de riesgo de proveedores.
6. **Seguridad:** Tenemos políticas, procedimientos y gobernanza establecidos que se mejoran permanentemente para salvaguardar la seguridad de los datos del cliente.
7. **Notificación de filtración:** Tenemos un proceso de respuesta a incidentes de seguridad documentado y evaluado.

1. Productos preparados para el GDPR

Uno de los aspectos fundamentales de nuestras líneas de trabajo para la aplicación es el respaldo a nuestros clientes al hacer que nuestros productos estén preparados para el GDPR. Con esa finalidad, ideamos requisitos mínimos de privacidad de datos / GDPR para nuestros productos. En línea con nuestro enfoque para fortalecer nuestras prácticas de privacidad de datos a nivel global, la mayoría de estos requisitos aplica a todos nuestros productos, no solo a aquellos productos que se encuentran disponibles en la UE. Esto también respalda a nuestros clientes fuera de la UE que pueden estar comprendidos por el alcance del GDPR.

Desarrollamos nuestros requisitos del producto de privacidad de datos / GDPR mediante un proceso sólido e intensivo. Generamos una versión inicial con asesoramiento externo. Durante múltiples sesiones de trabajo y revisiones con accionistas claves de nuestros equipos de desarrollo de producto y gestión de producto, perfeccionamos la versión hasta obtener requisitos del producto generales específicos y factibles con instrucciones detalladas. Los requisitos del producto de privacidad de datos / GDPR se convirtieron posteriormente en acciones específicas del producto en los planes de aplicación del producto para cada grupo de producto.

Nuestros requisitos del producto[16] se pueden categorizar de la siguiente manera:

Transparencia

- Capacidad de que los clientes accedan a enlaces con sus políticas / avisos de privacidad
- Proveer información sobre cómo se suele usar la información personal en un producto

Minimización / eliminación de datos

- Revisión de productos para determinar campos innecesarios / opcionales.
- Revisión de productos para determinar oportunidades de uso de seudónimos o datos anónimos en lugar de información personal.
- Capacidad de eliminar información personal cuando lo solicitan los clientes (en los casos en que los clientes / usuarios no pueden eliminar los datos por su cuenta).

Derechos individuales generales

- Capacidad de proveer acceso a información personal y corregirla cuando lo solicite un individuo.
- Capacidad de eliminar información personal cuando lo solicite un individuo.

Derechos individuales en la UE

- Capacidad de lidiar con solicitudes de portabilidad de datos (derecho de individuos para recibir datos en formato legible por máquina en determinadas circunstancias).
- Capacidad de dejar de usar información personal (derecho a objetar / derecho a restringir en determinadas circunstancias)

Blackboard ya tiene programas definidos para nuestra seguridad de producto que tienen en cuenta el GDPR. Por lo tanto, no definimos requisitos de seguridad específicos adicionales para el GDPR.[17]

2. Privacidad por diseño

A medida que en el mundo de hoy se vuelve cada vez más complejo que los individuos mantengan el control de su información (ver nuestra publicación de blog del día de la privacidad sobre este tema), la privacidad por diseño y la responsabilidad se vuelven aún más importantes para mantener la confianza de los individuos, clientes y reguladores, y para documentar cómo cumple una organización con el GDPR. Por lo tanto, colocamos nuestro enfoque de privacidad por diseño en el centro de nuestro programa de privacidad de datos global / GDPR.

Para Blackboard, esta en una evolución y no una revolución. Siempre se han realizado revisiones jurídicas de prácticas y productos nuevos. Con nuestro enfoque de privacidad por diseño, se formalizan y se documentan mejor dichas revisiones.

Enfoque

- Se ha creado un proceso de privacidad por diseño documentado y una lista de verificación.
- Los grupos de producto y áreas funcionales incluyen la lista de verificación de privacidad por diseño en sus procesos de cambio.
- Cada cambio material en cómo se usa la información personal requiere que se complete la lista de verificación de privacidad por diseño. Si bien no es especialmente requerida por el GDPR, esta es la mejor práctica.
- La lista de verificación llevará a la evaluación del impacto de la protección de datos (DPIA) más detallada para el uso de información personal de alto riesgo (requisito del GDPR).

El diagrama de flujo a continuación visualiza el enfoque:

3. Transferencias de datos

El GDPR no trae consigo ningún cambio significativo respecto a cómo se puede transferir la información personal fuera de la EU / del EEE. Se mantienen las restricciones y los mecanismos de transferencia de datos actuales. Esto quiere decir que se permiten las transferencias de datos si se aplica un mecanismo de transferencia de datos aprobado por la UE, tal como el Escudo de privacidad UE-EUA o las cláusulas modelo aprobadas por la UE (acuerdos sobre transferencia de datos). Estos mecanismos garantizan la protección adecuada de información personal aun cuando se abandona la UE / el EEE. Continuaremos con nuestro enfoque de múltiples capas y redundante del cumplimiento de transferencia

de datos. Esto significa que se abordan los requisitos de transferencia de datos a través de múltiples medios para garantizar que las salvaguardas apropiadas para su información se encuentran en orden:

- **Hosting regional:** Tenemos una estrategia de hosting regional con casi todos los productos alojados en la UE y otros productos que se planea trasladar a las soluciones de hosting regional. Si bien el GDPR no requiere almacenamiento regional y no creemos que la localización de datos lleve a mejor seguridad o privacidad de datos,[18] comprendemos que muchos clientes de la UE prefieren que sus datos se almacenen en la UE.
- **Escudo de privacidad:** Blackboard tiene la Certificación del Escudo de privacidad UE-EUA que nos permite transferir datos personales legalmente a Estados Unidos.
- **Cláusulas modelo:** También usamos los acuerdos de «cláusula modelo» aprobados por la UE que nos permite transferir datos personales como es debido fuera del EEE en el grupo de empresas de Blackboard (Acuerdo de transferencia de datos del cliente),
- **Proveedores:** Se cuenta con contratos sólidos con proveedores y socios (por ejemplo, IBM, Amazon Web Services) para garantizar que los requisitos de transferencia de datos (y otras obligaciones de protección de datos) se transmitan a nuestros proveedores y socios.

Actualmente,[19] tenemos varios centros de datos regionales para respaldar la manipulación de datos en la UE destinados a nuestros clientes de la UE:

- Hosting gestionado (centros de datos de Blackboard): Centros de datos en Ámsterdam (Países Bajos) y Frankfurt (Alemania).
- Hosting en la nube (centro de datos de AWS) AWS regional en Frankfurt, Alemania (eu-central-1).

Los centros de datos de AWS cumplen con un host de certificaciones y requisitos de las ISO 27001 e ISO 27018, a SOC2, con cumplimiento del GDPR así como también de los requisitos locales, tal como el C5 alemán e IT-Grundschutz. [20]

Es importante comprender que si bien la información personal de los clientes se almacena en estos centros de datos, en el caso de la mayoría de los productos (los que incluyen Learn 9.1, Learn SaaS, Open LMS y Collaborate) destinados a los clientes de la UE, se puede requerir el acceso a estos datos desde fuera de la UE / del EEE para proveer los productos y servicios, por ejemplo, para un soporte de 24 horas. Dichas transferencias de datos están permitidas gracias a las certificación del Escudo de privacidad UE-EUA y las cláusulas modelo.

4. Contratos con clientes

La Directiva actual requiere que un controlador de datos tenga un contrato con el proveedor (procesador de datos), pero no establece el contenido del contrato en detalle. El GDPR es más prescriptivo e incluye una lista de contenido requerido.[21]

Nuestro apéndice de procesamiento de datos estándar actual incluye todos los puntos requeridos a continuación. Se incluye de forma automática para clientes en nuestro acuerdo maestro estándar que se encuentran comprendidos por el GDPR.

✓ Use datos personales solo como se indica.

✓ El personal debe firmar acuerdos de confidencialidad.

✓ Se tienen que adoptar medidas de seguridad apropiadas.

✓ Solo incorpore proveedores (subprocesadores)...

- Según lo autorice el controlador de datos (puede ser una autorización general).
- Que se requiera por contrato que cumplan con las mismas obligaciones de protección de datos.

✓ Asista al controlador en la respuesta a solicitudes de derechos Individuales.

✓ Asista al controlador en medidas de seguridad, notificación de filtración y evaluaciones del impacto de la protección de datos.

✓ Devuelva o elimine datos al término del contrato.

✓ Provea información que sea necesaria para que el controlador de datos demuestre el cumplimiento.

✓ Informe inmediatamente al controlador de datos si alguna instrucción del controlador de datos incumple el GDPR.

5. Gestión de nuestros proveedores

Blackboard usa proveedores (por ejemplo, IBM, Amazon Web Services) para ayudarnos a proveer nuestros productos y servicios a nuestros clientes. En los casos en que esto requiere acceso a la información personal de nuestros clientes, Blackboard es responsable de las prácticas de privacidad de datos de los proveedores.

Como parte de nuestro programa del GDPR estamos conectando estrechamente el enfoque de privacidad por diseño con los procesos de gestión de riesgo de proveedores y adquisición. Esto tiene como resultado los siguientes controles clave:

- Contratos sólidos con un apéndice de privacidad y GDPR con terceros que imponen disposiciones materialmente equivalentes a las que tenemos vigentes con nuestros clientes.
- Acuerdos de «cláusula modelo» y/o apéndices de GDPR y Escudo de privacidad para permitir las transferencias de datos legales a nuestros proveedores.
- Política y marco de gestión de riesgo de proveedores documentados.
- Los proveedores nuevos con acceso a información personal tienen que completar un cuestionario de evaluación de seguridad de proveedores con preguntas sobre el cumplimiento de la privacidad de datos.
- Se requiere que los proveedores con acceso a sistemas gestionados por Blackboard cumplan con las políticas de identificación y autorización, y el control de acceso interno de Blackboard, para incluir revisiones de cuentas, según sea apropiado.
- Los proveedores tienen que acceder a los recursos de Blackboard mediante mecanismos aprobados (por ejemplo, VPN).
- Los proveedores tienen controles de acceso restringido en tráfico, usuarios y activos.

6. Seguridad

El GDPR no cambia materialmente las medidas técnicas y operativas (TOM, por sus siglas en inglés) para la seguridad de la información personal. Dichas medidas tienen que ser «adecuadas» al riesgo que implica de conformidad con la Directiva actual. Por lo tanto, seguimos confiando en nuestros programas establecidos de seguridad de la información.

Regulación del riesgo de seguridad de la información

Tenemos requisitos de política, procedimientos, gobernanza y técnicos establecidos para gestionar el riesgo de seguridad informática en el negocio.

Desde el primer día, el personal de Blackboard debe entender su responsabilidad de protección de los datos personales del cliente:

- Reconocer política para proteger información delicada
- Capacitación anual sobre seguridad y privacidad de datos del usuario
- Ejercicios de *phishing* [fraude electrónico]
- Boletines de sensibilización

Los siguientes requisitos se ponen en práctica para la protección de datos por parte de nuestro personal:

- Se definen las clasificaciones de datos con requisitos para la protección de cada tipo de dato. Los datos de nuestro cliente, los datos de las instituciones y sus alumnos son de máxima sensibilidad.
- Se ponen en práctica los controles técnicos para salvaguardar los datos, por ejemplo:
  - uso de codificación
  - actualizaciones de seguridad rápidas
  - controles de autenticación mejorados
  - protección contra tráfico de internet y correos electrónicos maliciosos
  - tecnologías de protección de punto final
  - acceso restringido con base al principio de mínimo conocimiento

No es solo el GDPR ...

Como una empresa global al servicio de la comunidad educativa, monitoreamos de cerca las leyes y reglamentaciones de seguridad y privacidad de datos específicas del sector de la educación y geográficamente pertinentes.

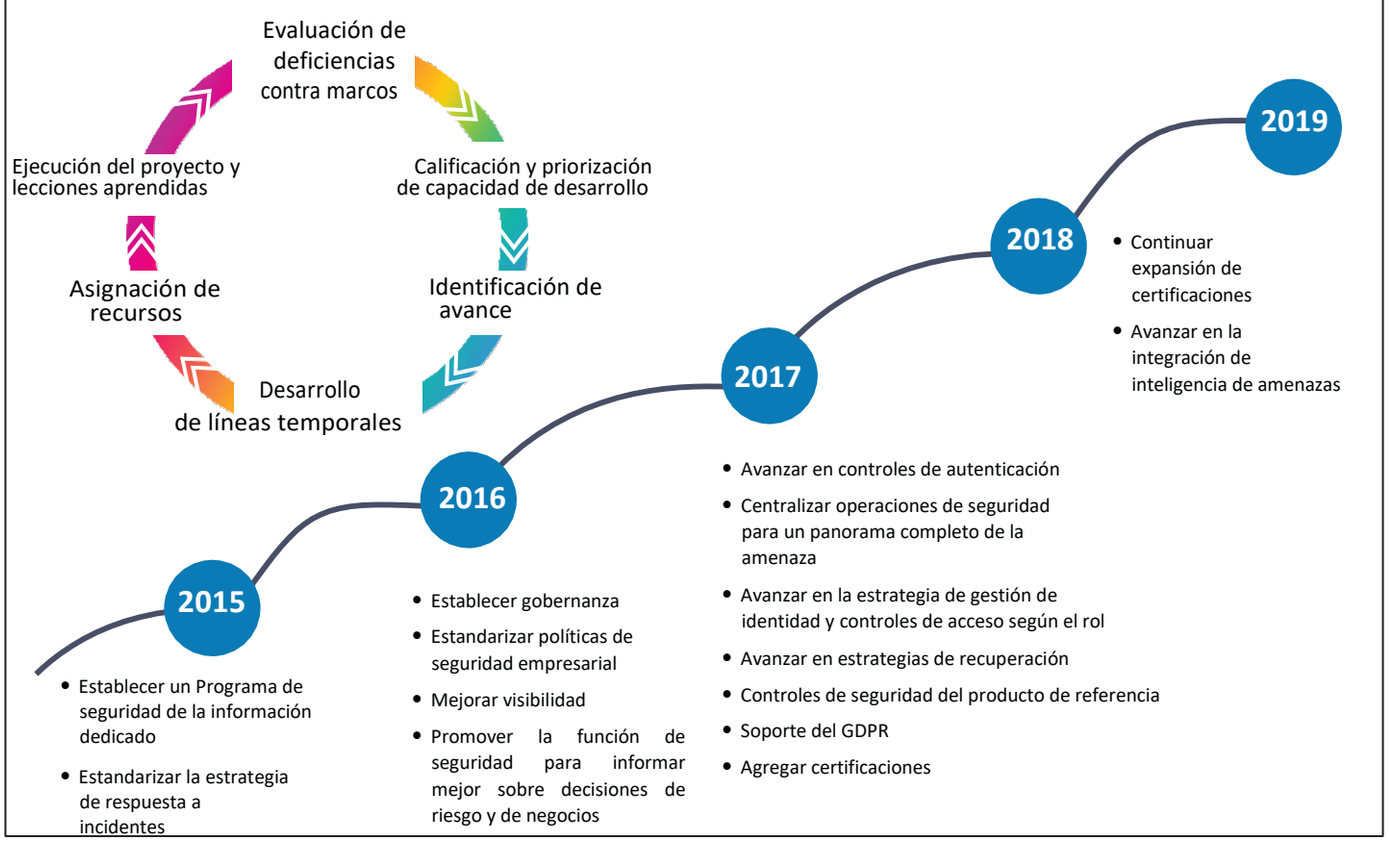
En la lista, a continuación, figuran algunos ejemplos de reglamentaciones de seguridad y privacidad de datos, estándares y marcos que Blackboard tiene en cuenta además del GDPR cuando desarrollamos nuestras políticas de seguridad, procesos y controles técnicos.

- Ley de derechos educativos y privacidad familiar de Estados Unidos (FERPA, por sus siglas en inglés), Enmienda a la protección de los derechos del alumno (PPRA, por sus siglas en inglés).
- Ley de protección de la privacidad infantil en internet de Estados Unidos (COPPA, por sus siglas en inglés)
- Leyes estatales de Estados Unidos (mosaico de 50 estados existentes y emergentes)
- Estándares del gobierno de Estados Unidos – FedRAMP
- Estándares de seguridad de datos de PCI, según corresponda
- ISO/IEC, OWASP, NIST
- Estándares internacionales (MTCS, IRAP)

Análisis de desarrollo de seguridad y planes de trabajo

Trabajamos duro para mejorar permanentemente nuestras medidas de seguridad técnica y operativa. El diagrama en la siguiente página visualiza nuestros análisis de desarrollo permanente y nuestros planes de trabajo.

Adopción de marcos: Análisis de desarrollo de seguridad y planes de trabajo



7. Notificación de filtración

Uno de los cambios fundamentales del GDPR es la nueva notificación obligatoria sobre filtraciones de datos personales a la autoridad de protección de datos competente y (en algunos casos) a los individuos afectados.[22]

En el caso de la mayoría de nuestros productos y servicios, Blackboard es un procesador de datos[23] conforme al GDPR. La obligación de notificar a las autoridades de protección de datos e individuos en caso de una filtración que involucre a Blackboard recaería, por lo tanto, en nuestros clientes. Sin embargo, el GDPR requiere que los procesadores de datos como Blackboard notifiquen a sus clientes (controladores de datos) sin demora injustificada (es decir, «rápidamente»)[24] en dicho caso.

Tenemos las siguientes medidas en vigencia que respaldan a nuestros clientes en el cumplimiento de sus obligaciones en el caso de una filtración de datos personales en Blackboard con relación al cliente:

- Proceso de respuesta a un incidente de seguridad (SIR) de Blackboard
  - Documentado y habitualmente evaluado
  - Facilita la identificación, investigación y compensación rápidas en caso de un incidente
  - Permite proveer notificaciones rápidas a los clientes
  - Confía en el equipo establecido de respuesta a incidentes de seguridad (el que incluye al Director de seguridad de información y al Director de privacidad global)
- Nuestra obligación de notificar a los clientes de manera rápida se establece expresamente en nuestro acuerdo maestro estándar y en el apéndice de protección de datos.[25]

CONCLUSIÓN

El GDPR requiere cambios significativos con impacto más allá de la fecha de cumplimiento del 25 de mayo de 2018. Esperamos que este libro blanco pueda contribuir a su aplicación con éxito del GDPR y que haya demostrado qué tan seriamente Blackboard considera al GDPR y al cumplimiento de la privacidad de datos.

Las siguientes secciones proveen información adicional útil y enumeran nuestro correo electrónico de contacto si tiene alguna duda o comentario sobre este libro blanco.

RECURSOS ÚTILES DEL GDPR

Los recursos con enlaces que figuran a continuación son solo una pequeña selección de material útil que se encuentra disponible en internet. No pretende ser una lista exhaustiva.

Por un análisis detallado de cómo el GDPR aplica a usted, también debería solicitar el asesoramiento de especialistas. Es importante que confíe en expertos en la protección de datos con experiencia (por ejemplo, pertenecientes al estudio jurídico de su preferencia).

Recursos de la UE oficiales

- Texto del GDPR
- Pautas del Grupo de trabajo del artículo 29
- Sitio web de la Comisión de la UE para el GDPR

Material sobre la Autoridad de protección de datos de la UE

- La Oficina del comisionado de información (ICO, por sus siglas en inglés) de Reino Unido tiene un excelente sitio web para el GDPR con material útil en lenguaje simple que se actualiza de forma permanente.
- El Comisionado de protección de datos (DPC, por sus siglas en inglés) de Irlanda tiene una página dedicada al GDPR para organizaciones.
- La CNIL de Francia provee algo de material en inglés que incluye un software gratuito de Evaluación del impacto de la privacidad (y mucho más material en francés).
- La AEPD de España confeccionó una guía para instituciones educativas (PDF, en español).

Guías de estudios jurídicos

- Guía de Bird & Bird para el GDPR
- Rastreador de leyes de Estados miembros de Bird & Bird (seguimiento de variaciones del GDPR a nivel nacional)
- Guía de supervivencia al GDPR de Linklaters (PDF)
- Manual del GDPR de White & Case

Otras organizaciones

- JISC Reino Unido tiene recursos, eventos y actualizaciones de blogs útiles sobre el GDPR
- UCISA ha publicado un documento sobre la mejor práctica del GDPR con etapas prácticas y casos de estudio
- La Asociación internacional de profesionales en privacidad (IAPP, por sus siglas en inglés) tiene un buen boletín semanal (gratuito) sobre las novedades en privacidad de datos en Europa.
- La IAPP también tiene un útil resumen de proveedores de herramientas de privacidad de datos (PDF)
- Amazon Web Services tiene un Centro dedicado al GDPR

BIOGRAFÍAS

Stephan Geering

Director de privacidad global

- Responsabilidad global de cumplimiento de leyes sobre seguridad y privacidad de datos.
- Lidera el programa de aplicación de privacidad de datos global / GDPR.
- Responde al Director jurídico, miembro del equipo jurídico de Blackboard.
- Reside en Londres.

Antecedentes de Stephan:

- Abogado / Subcomisionado de protección de datos en una Autoridad para la protección de datos cantonal suiza (2002-2008)
- LLM en University College de Londres (2008-2009)
- Director asociado, Privacidad del grupo en Barclays (2010-2012)
- Encargado regional para EMEA de operaciones de privacidad de datos en Citigroup (2012-2014)
- Director ejecutivo de privacidad para EMEA y APAC en Citigroup (2014-2017)
- Certificación CIPP/E

Rebecca McHale

Directora ejecutiva de seguridad de información

- Lidera la estrategia de seguridad para productos e infraestructura
- Supervisa la gobernanza de ciberseguridad de Blackboard
- Responde al Director de producto
- Reside en Washington, D.C.

Antecedentes de Rebecca:

- Se unió a Blackboard en 2016; recientemente combinó los equipos de seguridad y mejoró la organización de la seguridad en la empresa
- MS en Matemática discreta y aplicaciones informáticas en Royal Holloway, University of London
- Previamente, Directora Senior para los Programas de seguridad cibernética en Novetta y CSRA al servicio del gobierno de Estados Unidos y clientes comerciales, por ejemplo, Departamento de Estado, Administración de seguridad en el transporte (TSA, por sus siglas en inglés) y Corporación Federal de Seguro de Depósitos (FDIC, por sus siglas en inglés)

MÁS INFORMACIÓN

Puede encontrar más información en nuestra página destinada a la Comunidad de seguridad y privacidad de datos.

También tenemos un boletín informativo sobre privacidad de datos. Si quisiera recibir nuestro boletín informativo o si tiene alguna duda o comentario sobre este libro blanco, puede contactarnos en privacy@blackboard.com.

Fuentes

1 Ver el final de la sección «Recursos útiles del GDPR» por más guías detalladas sobre el GDPR.

2 Se prefiere la expresión «información personal» a «datos personales» pero se usa con el mismo significado y alcance que «datos personales».

3 El controlador de datos es la organización que determina los medios y fines del procesamiento de datos (cómo y por qué se usa la información personal).

4 Ver la sección «El papel de nuestra organización y la suya conforme al GDPR».

5 Ver la sección «Desmitificación del GDPR» más adelante por más detalles sobre las transferencias de datos.

6 Ver «Una introducción a la ley de protección de datos» de la ICO por una síntesis útil de la ley.

7 Ver también las publicaciones del blog de la ICO de Reino Unido sobre Mitos del GDPR.

8 Ver también las Pautas del WP29 (borrador) sobre consentimiento conforme a la reglamentación 2016/679 (WP259) y las pautas de la ICO sobre consentimiento.

9 Pautas del WP29 sobre notificaciones de filtración de datos personales conforme a la reglamentación 2016/679 (WP250rev.01).

10 Ver también la sección «Transferencias de datos».

11 Ver, por ejemplo, Prepararse para el GDPR – 12 pasos a dar ahora de la ICO de Reino Unido (PDF).

12 Ver también la sección «Desmitificación del GDPR».

13 Ver la sección «Recursos útiles del GDPR».

14 Por más información sobre el Director de privacidad global y la Directora de seguridad de información ver la sección de Biografía.

15 Como parte del proyecto de certificación del Escudo de privacidad UE-EUA, ya incluimos las disposiciones contractuales del GDPR necesarias en muchos de los contratos con nuestros proveedores (subprocesadores) que tienen acceso a información personal de la UE.

16 Cabe destacar que no todos los requisitos del producto aplican a todos los productos. Por ejemplo, algunos productos no tienen una interfaz de usuario que permitiría a los clientes acceder a enlaces con sus políticas / avisos de privacidad.

17 Ver la sección «Seguridad» por más detalles.

18 Una vez que la red o el sistema se conecta a internet, la ubicación física de los datos tiene poco o ningún impacto en las amenazas de seguridad. Ver el libro blanco de Amazon Web Services (AWS) «Perspectiva de la política de AWS sobre residencia de datos» (en particular las páginas 2 y 3) por argumentos convincentes contra la localización de datos.

19 A la fecha de este documento.

20 Ver los Programas de cumplimiento de AWS por la lista completa de certificaciones y cumplimiento legal.

21 Art. 28(2)-(4) del GDPR.

22 Art. 33 y 34 del GDPR.

23 Por una explicación del papel del procesador de datos, ver la sección «El papel de nuestra organización y la suya conforme al GDPR».

24 Ver la sección «Desmitificación del GDPR» precedente por más detalles sobre plazos y procesos de notificación de filtración de datos personales.

25 Ver también la sección «Contratos con clientes»

Blackboard.com