كيف يساهم تنفيذ Blackboard للائحة العامة لحماية البيانات في دعم عملائنا

تمثل اللائحة العامة لحماية البيانات للاتحاد الأوروبي تغييرًا جذريًا. وترحب بلاك بورد Blackboard بهذا التغيير. إننا نهتم بخصوصية البيانات ونتفهم أنها حقٌ من حقوق الإنسان. تعزز اللائحة العامة لحماية البيانات حقوق الأفراد وسيترتب عليها ممارسات أفضل لخصوصية البيانات. وذلك من شأنه أن يفيد الأفراد والمؤسسات نظرًا لأنه يزيد من الثقة بينهم.

إننا ننشر هذه الورقة لتزويد عملائنا بنبذة عن التغييرات والخرافات المثارة حول اللائحة وذلك لتوضيح النهج الذي نتبعه في تنفيذها وعرض لكيفية دعم ما نبذله من جهود لمؤسستك بالتفصيل. نركز على المعلومات التي نرى أنها ستكون مفيدة للغاية بالنسبة لك. ولذلك تعد هذه الورقة البيضاء بمثابة دليل شامل للائحة العامة لحماية البيانات بجميع المقاييس.[1]

تجلب اللائحة تغييرات جوهرية لكننا في Blackboard يمكننا البناء على ما لدينا من ممارسات قوية لخصوصية البيانات (على سبيل المثال، اعتماد درع الخصوصية الأوروبي الأمريكي). إننا نرى أن اللائحة تعد بمثابة فرصة لمزيد من التعزيز لممارساتنا، وسنواصل تركيزنا على العملاء ودعمنا لكم فيما يتعلق بالالتزام بخصوصية البيانات.

هذه المواد معدة لأغراض معلوماتية فقط ولا تعد مشورة قانونية. برجاء طلب مشورة المحاميين الداخليين أو الخارجيين التابعين لك لتنفيذ اللائحة العامة لحماية البيانات داخل مؤسستك وما يرتبط بذلك من استفسارات قانونية.

المحتويات

اللائحة العامة لحماية البيانات- ما تحتاج إلى معرفته

اللائحة العامة لحماية البيانات هي التشريع الأوروبي الجديد لحماية البيانات الذي سيحل محل التوجيه الأوروبي الحالي لحماية البيانات 46/96 (التوجيه)، وتنفيذ قوانين حماية البيانات في الدول الأعضاء بالاتحاد الأوروبي (كقانون حماية البيانات بالمملكة المتحدة 1998)،

صدرت اللائحة العامة لحماية البيانات في مايو 2016 بتاريخ التزام يوافق 25 مايو 2018.

في الأقسام التالية، نقدم نبذة مختصرة (لا مفصلة) عن شروط اللائحة العامة لحماية البيانات. يمكنك العثور على روابط عن المزيد من الإرشادات التفصيلية في قسم " الموارد المفيدة للائحة العامة لحماية البيانات".

لماذا قانون جديد؟

اقتنع المشرعون والمنظمون في الاتحاد الأوروبي أن التوجيه بحاجة إلى التحديث لمعالجة عدم الانسجام والتطورات المجتمعية والتكنولوجية في العشرين سنة التي مرت على التوجيه. كان على رأس القائمة صلاحيات إنفاذ أقوى ووصول أوسع نطاقًا وتعزيز حقوق الأفراد.

تستهدف العديد من الأحكام الجديدة (كالتأثير الخارجي) في المقام الأول شركات وسائل التواصل الاجتماعي والإنترنت خارج الاتحاد الأوروبي. شعر المشرعون والمنظمون بالاتحاد الأوروبي أن التوجيه القائم لا يوفر القدر الكافي من حماية حقوق خصوصية البيانات الخاصة بمواطني الاتحاد الأوروبي الذين يستخدمون هذه الخدمات الخاصة بوسائل التواصل الاجتماعي والإنترنت.

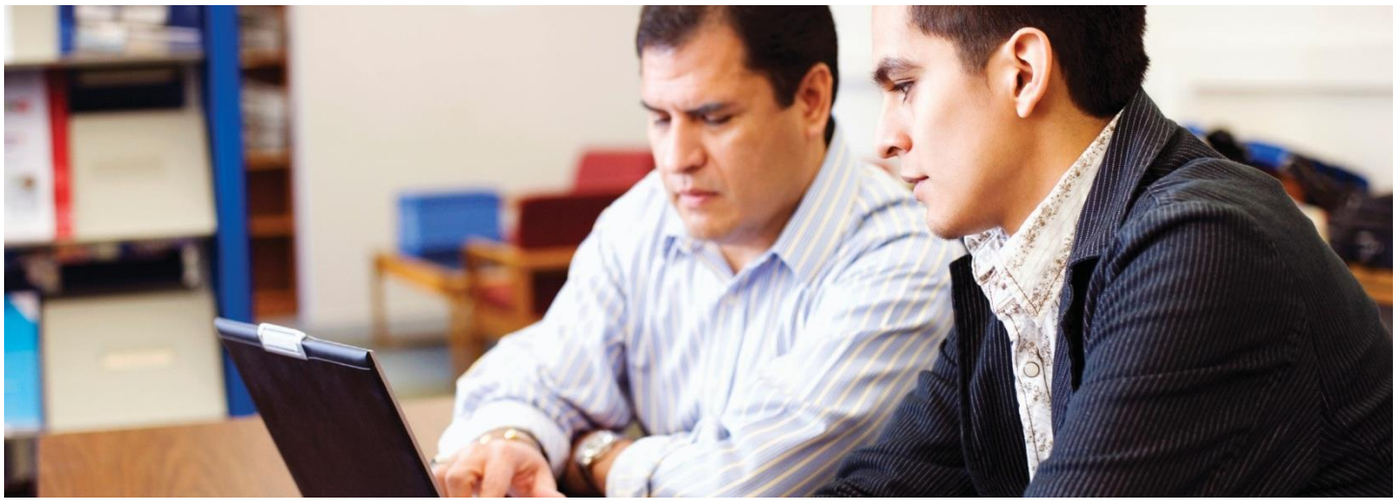
تعمل Blackboard بشكل مختلف عن شركات وسائل التواصل الاجتماعي وغيرها من شركات الإنترنت القائم نموذجها على "تنقيد" بيانات المستخدمين. إننا نجمع المعلومات الشخصية[2] لعملائنا ونستخدمها بتوجيه منهم لتزويدهم ومستخدميهم بمنتجاتنا وخدماتنا. ولا نجمع المعلومات الشخصية أو نستخدمها لبيعها أو لبيع الإعلانات. نتفهم أن المعلومات الشخصية قد عُهد بها إلينا وأن ذلك يعود علينا بالتزامات. لذلك لدينا مصلحة ومسؤولية مشتركة مع عملائنا في حماية هذه المعلومات.

تعد Blackboard معتمدة بموجب اتفاق "درع الخصوصية" كما تفخر بالتوقيع على "تعهد خصوصية الطلاب" وهي عضو في "منتدى مستقبل الخصوصية".

Privacy Shield Certified

STUDENT PRIVACY PLEDGE SIGNATORY

FUTURE OF PRIVACY FORUM



ما هو الجديد؟

في حين، واستنادًا إلى المبادئ والمفاهيم الأوروبية القائمة لخصوصية البيانات، تُدخل اللائحة العامة لحماية البيانات تغييرات جوهرية على نظام خصوصية البيانات في الاتحاد الأوروبي بما فيها:

- زيادة صلاحيات التغريم حتى 4% من معدل الدوران العالمي أو 20 مليون يورو (أيهما أكبر)
- توسيع النطاق الإقليمي للمؤسسات العاملة خارج الاتحاد الأوروبي التي تقدم المنتجات والخدمات للمقيمين داخل دول الاتحاد الأوروبي أو التي تراقبهم
- الإشعار الإلزامي بالخروقات للسلطات الإشرافية في خلال 72 ساعة لمراقبي البيانات[3]
- شروط أكثر صرامة فيما يتعلق بالموافقة
- تعزيز حقوق الأفراد (بما فيها الحق في مسح البيانات وإمكانية نقلها)

إلا أن بعض أهم التغييرات تتمثل في مبادئ المساءلة والخصوصية الجديدة حسب التصميم. تتطلب هذه المبادئ الإدارة والإجراءات الفعالة لخصوصية البيانات وكذلك توثيق أكثر تفصيلاً وفعالية عن كيفية التزام أي مؤسسة بشروط اللائحة العامة لحماية البيانات.

ما يبقى على حاله؟

تظل العديد من المفاهيم والتعاريف الواردة في اللائحة العامة لحماية البيانات كما هي أو مشابهة مقارنةً بالتوجيه:

- يظل تعريف "البيانات الشخصية" (أو المعلومات الشخصية) بشكل عام كما هو لكنه يشمل صراحةً الآن عناوين IP وملفات تعريف الارتباط ومعرفات الأجهزة
- تظل مفاهيم "مراقب البيانات" و"معالج البيانات" كما هي (إلا أن اللائحة العامة لحماية البيانات تفرض مزيدًا من المسؤوليات المباشرة على معالجي البيانات)[4]
- يتم الإبقاء على المبادئ الأساسية لمعالجة البيانات الواردة في التوجيه (كالمعالجة القانونية والنزيهة والحد من الأغراض والاحتفاظ بالبيانات الشخصية فقط ما دامت ضرورية)
- تظل شروط نقل البيانات بشكل عام كما هي: يُسمح بعمليات نقل البيانات خارج الاتحاد الأوروبي/المنطقة الاقتصادية الأوروبية مادامت تُستخدم آلية معتمدة لنقل البيانات (كدرع الخصوصية الأوروبي الأمريكي أو "الشروط النموذجية")[5]

يعني المستوى الأعلى من الغرامات بموجب اللائحة العامة لحماية البيانات أن عدم الالتزام بالمبادي والشروط القائمة كالاحتفاظ بالبيانات الشخصية فقط مادامت ضرورية أو اتخاذ تدابير أمنية مناسبة من المرجح أن يحمل مخاطر متزايدة.

ما تأثير خروج بريطانيا من الاتحاد الأوروبي؟

ستطبق اللائحة العامة لحماية البيانات مباشرةً في المملكة المتحدة اعتبارًا من 25 مايو 2018 حتى "الخروج من الاتحاد الأوروبي" بنهاية مارس 2019. إلا أنه حتى بعد هذا الخروج، سترسي اللائحة العامة لحماية البيانات المعايير للمملكة المتحدة:

- لقد نشرت حكومة المملكة المتحدة قانون حماية البيانات لسنة 2017 (قيد التشريع حاليًا) الذي ينفذ اللائحة العامة لحماية البيانات قبل الخروج من الاتحاد الأوروبي وبعده[6]
- بعد خروج بريطانيا من الاتحاد الأوروبي، تنطبق اللائحة العامة لحماية البيانات مباشرة على المؤسسات العاملة بالمملكة المتحدة التي توفر السلع والخدمات للمقيمين بالاتحاد الأوروبي أو التي تراقبهم (كجامعات المملكة المتحدة التي ينشط بها استقدام طلاب من الاتحاد الأوروبي)

التأثير على عمليات نقل البيانات من وإلى المملكة المتحدة:

- لقد أوضح الاتحاد الأوروبي أنه سيتم اعتبار المملكة المتحدة عقب خروج بريطانيا من الاتحاد الأوروبي "بلد ثالث"، ما يعني عدم اعتبارها بلد "ملائم" (مدرج ضمن القائمة البيضاء) لعمليات نقل البيانات بعد الآن.
- مالم وحتى تعلن المفوضية الأوربية المملكة المتحدة كبلد ملائم لعمليات نقل البيانات (كجزء من اتفاق انتقالي)، يجب تطبيق اتفاقيات نقل البيانات أو غيرها من آليات نقل البيانات وذلك لنقل المعلومات الشخصية من الاتحاد الأوروبي إلى المملكة المتحدة.
- في المقابل، يجب على المملكة المتحدة تحديد الدول التي تعتبرها ملائمة لنقل البيانات (والتي من المحتمل أن تشمل دول الاتحاد الأوروبي والدول المدرجة ضمن القائمة البيضاء من جانب الاتحاد الأوروبي). وفيما يتعلق بالدول التي لا تعتبر ملائمة لنقل البيانات، سيقتضي الأمر استخدام آليات نقل البيانات المعترف بها داخل المملكة المتحدة (التي قد تكون مشابهة لآليات الاتحاد الأوروبي) لعمليات نقل المعلومات الشخصية خارج المملكة المتحدة.

تبسيط اللائحة العامة لحماية البيانات

كان أحد أهداف اللائحة العامة لحماية البيانات توفير المزيد من الوضوح من خلال المزيد الوصف التفصيلي. إلا أنه لا يزال هناك العديد من جوانب اللائحة العامة لحماية البيانات مفتوحة للتأويل. بالإضافة إلى ذلك، لقد أدى تعقيد اللائحة العامة لحماية البيانات إلى عدم فهمها وكذلك البيانات المبالغ فيها. وقد ترتب على ذلك ظهور العديد من الخرافات قمنا بنشر القليل منها فيما يلي:[7]

الخرافة الأولى: **اشتراط الموافقة على جميع عمليات معالجة المعلومات الشخصية**

الحقيقة: الموافقة هي مجرد أحد الأسس القانونية العديدة التي تسمح بمعالجة المعلومات الشخصية (كالمعالجة المطلوبة لأداء عقدٍ ما أو "مصلحة مشروعة" لمؤسسة ما). لقد أصبحت شروط منح الموافقة مشددة جدًا. على سبيل المثال، ما لم يكن الأفراد يملكون حرية اختيار حقيقية ويمكنهم سحب موافقتهم في أي وقت دون أي عواقب، فلن تعتبر موافقة صحيحة. ستكون الأسس القانونية الأخرى مناسبة أكثر في العديد من سيناريوهات معالجة البيانات.[8]

الخرافة الثانية: **تنطبق فترة الـ 72ساعة للإشعار بالخروقات على سلسلة التوريد بأكملها (أي من لحظة علم أي معالج (ثانوي) بالخرق)**

الحقيقة: تشترط اللائحة العامة لحماية البيانات على معالجي البيانات إشعار مراقب بياناتهم "دون تأخير غير مبرر" في حالة خرق البيانات الشخصية. بمجرد قيام معالج البيانات بإشعار المراقب، هل تبدأ فترة الـ 72ساعة الخاصة بإشعار مراقب البيانات. المادة 29 مجموعة العمل، لقد أوضحت مجموعة سلطات حماية البيانات بالاتحاد الأوروبي في مبادئها التوجيهية النهائية[9] أن عبارة "بدون تأخير غير مبرر" تعني الإشعار "السريع" (لا الإشعار "الفوري" كما اقتُرح في مسودة سابقة).

الخرافة الثالثة: **عمليات نقل البيانات خارج الاتحاد الأوروبي/المنطقة الاقتصادية الأوروبية محظورة أو مسموحة فقط بموافقة العميل على كل عملية من عمليات نقل البيانات**

الحقيقة: تُبقي اللائحة العامة لحماية البيانات بشكل عام على الشروط القائمة لنقل البيانات. على هذا النحو، يُسمح بعمليات نقل البيانات في حالة تطبيق آلية أوروبية معتمدة لنقل البيانات كدرع الخصوصية الأوروبي الأمريكي أو الشروط النموذجية المعتمدة من الاتحاد الأوروبي (اتفاقيات نقل البيانات). لقد طبقت Blackboard هذه الآليات لنقل المعلومات الشخصية للعملاء وفقًا للشروط.[10] ونظرًا أن Blackboard تعمل كمعالج بيانات، هناك حاجة إلى تعليمات عامة لعمليات نقل البيانات من العميل (الواردة في اتفاقية معالجة البيانات القياسية الخاصة بنا)، إلا أن موافقات العميل على كل عملية من عمليات نقل البيانات ليست ضرورية.

الخرافة الرابعة: **يقتضي حق المسح من المؤسسات حذف جميع بيانات أي فرد**

الحقيقة: حق المسح الجديد ليس "بحق مطلق للنسيان". بل إنه حق لحذف البيانات ما لم تعد مطلوبة وفي ظروفٍ أخرى، مالم تستوفي المؤسسة شروط اللائحة العامة لحماية البيانات. إذا كانت أي مؤسسة لاتزال في احتياج إلى الاحتفاظ بالبيانات بشكل مشروع (على سبيل المثال، بسبب شروط الاحتفاظ بالسجلات)، فإنه لا داعي إلى حذف هذه المعلومات الشخصية.

الخرافة الخامسة: **اللائحة العامة لحماية البيانات تنطبق على جميع الجامعات التي بها طلاب من دول الاتحاد الأوروبي**

الحقيقة: لا يكفي وجود طلاب مقيدين من دول الاتحاد الأوروبي حتى تُطبق اللائحة العامة لحماية البيانات. تنطبق اللائحة العامة لحماية البيانات على المؤسسات التعليمية المؤسسة في الاتحاد الأوروبي. كما تنطبق على الجامعات الموجودة خارج الاتحاد الأوروبي ولكن فقط إذا كانت تقدم سلع وخدمات للأفراد المقيمين في دول الاتحاد الأوروبي أو تراقب سلوكياتهم. يقتضي "تقديم الخدمات" التي يتعين النظر فيه درجة معينة من الاستهداف. الحقيقة المجردة بأن طلاب دول الاتحاد الأوروبي مقيدون تعد غير كافية. إلا أنه قد تنطبق اللائحة العامة لحماية البيانات حال استهداف الجامعات للمقيمين في دول الاتحاد الأوروبي بشكل فعال (على سبيل المثال للدورات عبر الإنترنت) أو استقدام طلاب في دول الاتحاد الأوروبي بشكل فعال. هذه المعايير مفتوحة للتأويل. نوصي بحصول العملاء على المشورة القانونية.

تنفيذ اللائحة العامة لحماية البيانات

لماذا من المهم الحصول على حق خصوصية البيانات واللائحة العامة لحماية البيانات

بالتأكيد أن مخاطر غرامات معدل الدوران العالمي البالغة 4% أحد الأسباب وراء بدء تعامل العديد من المؤسسات مع خصوصية البيانات بجدية أكبر. إلا أننا نعتقد أن الحالة الإيجابية للممارسات الجيدة لخصوصية البيانات تتمثل في أنها على الأقل مقنعة نظرًا أن خصوصية البيانات حقٌ من حقوق الإنسان وأن امتلاك ممارسات قوية لخصوصية البيانات يولد الثقة.

تتميز المعلومات الشخصية في مجتمع اليوم بأنها في كل مكان. وعادةً ما يُطلق على المعلومات الشخصية النفط الجديد للاقتصاد. إننا جميعًا نستخدم الخدمات عبر الإنترنت ونسلم معلوماتنا الشخصية. لكن دراسة بعد دراسة تظهر أن المؤسسات تكون غير موثوق بها عندما يتعلق الأمر بالمعلومات الشخصية. هناك شعور بأن الأفراد قد فقدوا السيطرة على بياناتهم. يستجيب المشرعون والمنظمون لذلك. وعلى الأرجح أن اللائحة العامة لحماية البيانات هي المثال الأبرز على ذلك.
تحتاج المؤسسات إلى استعادة ثقة الأفراد. الممارسات الجيدة لخصوصية البيانات هي المفتاح لبناء هذه الثقة. هناك أيضًا ميزة تنافسية. وأخيرًا، إنها أيضًا تساعد المؤسسات على الابتكار. إذا كان الطلاب (والعاملون) يثقون في مؤسستك، فإنهم على الأرجح سيشاركون معلوماتهم وسيستخدمون أدوات جديدة.

يمكن أن يكون التعامل مع خصوصية البيانات بشكل خاطئ كارثيًا. إن خروقات البيانات أمر معتاد أن تسمع عنه في الأخبار. يلي ذلك تدمير السمعة وفقدان ثقة الأفراد ومخاطر المطالبات من أولئك التي أسيئ إدارة بياناتهم. قد لا تستخدم سلطات حماية البيانات حق فرض غرامات على معدل الدوران بنسبة 4% من البداية، لكنها تمتلك العديد من أدوات الإنفاذ الأخرى تحت تصرفها ويمكنها إرغام المؤسسات على تغيير ما يطبقونه من ممارسات البيانات وتنفيذ برامج خصوصية البيانات مصحوبة بعمليات تدقيق خارجية دورية.

دورنا ودور مؤسستك بموجب اللائحة العامة لحماية البيانات

تُبقي اللائحة العامة لحماية البيانات على مفهوم "مراقب البيانات" و"معالج البيانات". هذا المفهوم بالغ الأهمية نظرًا أنه يحدد مسؤوليات المؤسسات ومقدمي الخدمات لهم والتزاماتهم القانونية.

إن أي مؤسسة بمثابة مراقب بيانات إذا ما حددت "وسائل وأغراض" معالجة المعلومات الشخصية، أي سبب استخدام المعلومات وكيفية القيام بذلك. من ناحية أخرى، معالج البيانات هو مؤسسة تعمل نيابةً عن مراقب البيانات وفي ضوء توجيهاته.

بالنسبة لمعظم منتجات Blackboard وخدماتها (على سبيل المثال، ليرن، كولابورايت، مودلرومز)، تعتبر Blackboard معالج بيانات وعملاؤنا مراقب البيانات.

تفرض اللائحة العامة لحماية البيانات المزيد من الشروط المباشرة على معالجي البيانات مثل Blackboard. إلا أن غالبية شروط هذه اللائحة لا تزال مطبقة على مراقبي البيانات (على سبيل المثال مسؤولية إبلاغ الأفراد بكيفية استخدام بياناتهم والالتزام بطلبات الأفراد للوصول إلى بياناتهم والإشعار الإلزامي لسلطات حماية البيانات والأفراد بخرق البيانات).

ما الذي يمكنك فعله للاستعداد للائحة العامة لحماية البيانات؟

يتعين أن تكون جميع المؤسسات في نطاق اللائحة العامة لحماية البيانات جاهزة بحلول 25 مايو 2018. فيما يلي بعض الأشياء الرئيسية التي يمكن للعملاء القيام بها لتجهيز أنفسهم. هذه القائمة من الخطوات قائمة على تجربتنا الخاصة ولا يُقصد تعميمها بأي حال من الأحوال. يُرجى التأكد من الاستعانة بخبراء في خصوصية البيانات لمساعدتك في التنفيذ. كما أصدرت العديد من سلطات حماية البيانات إرشاداتها حول كيفية تنفيذ اللائحة العامة لحماية البيانات.[11]

نأمل أن تكون قد أنجزت بالفعل الخطوات الستة الأولى وأن تكون حاليًا في منتصف تنفيذ خطط عملك. لكن الأوان لم يفت أبدًا للبدء. حتى وإن كنت قد بدأت للتو، يمكنك تنفيذ التغييرات الأكثر أهمية. كما يعني ذلك أنك ستكون قادرًا على أن تثبت لسلطة حماية بياناتك أن تعمل على خطة. تجاهل اللائحة العامة لحماية البيانات ليس بخيارٍ وارد.

1. **التحقق مما إذا كانت اللائحة العامة لحماية البيانات تنطبق على مؤسستك**

إذا تأسست مؤسستك في الاتحاد الأوروبي، فإن اللائحة العامة لحماية البيانات تنطبق. لكن اللائحة قد تنطبق أيضًا على المؤسسات خارج الاتحاد الاوروبي.[12]

2. **إنشاء مشروع للائحة العامة لحماية البيانات**

صمم ونفذ مشروع مخصص للائحة العامة لحماية البيانات. عادةً ما تتلقى الدعم لإدارة المشروع وستُرشح لك جهات اتصال بإمكانها دعمك في كل قسم. سيمتد هذا المشروع ليشمل جميع الأقسام في مؤسستك وستحتاج إلى مساعدة.

3. **ترشيح خبير في اللائحة العامة لحماية البيانات لإدارة المشروع**

لا ينبغي للخبير أن يكون خبيرًا في خصوصية البيانات فحسب، بل أيضًا يمتلك الوقت والموارد وكذلك تأمين الدعم الخارجي (على سبيل المثال، شركة محاماة). إذا كانت مؤسستك هيئة عامة مؤسسة داخل الاتحاد الأوروبي، سيتعين عليك أيضًا تعيين مسؤول حماية بيانات.

4. **ضمان مشاركة الإدارة العليا وإشرافها**

من الصعب تنفيذ مشروع للائحة العامة لحماية البيانات دون دعم الإدارة العليا وتوجيهها وإشرافها.

5. **مراجعة استخدامك للمعلومات الشخصية وإجراء تحليل فجوات**

فهم مكان وكيفية استخدام المعلومات الشخصية ومكان الاحتياج إلى تحسينات اللائحة العامة لحماية البيانات المرحلة الرئيسية الأولى لمشروع اللائحة العامة لحماية البيانات.

6. **وضع خطط العمل لسد الفجوات**

على الأرجح أن هذا هو الجزء الأصعب من اللائحة العامة لحماية البيانات نظرًا أنه يتطلب ترجمة الشروط عالية-المستوى عادةً للائحة العامة لحماية البيانات إلى إجراءات محددة وعملية لجميع العمليات والأنظمة المختلفة.

7. **تنفيذ خطط العمل**

الثقة جيدة لكن السيطرة أفضل في هذه الحالة. تتطلب هذه المرحلة تتبع خطط عمل الآخرين للتأكد من استيفائهم للمواعيد النهائية.

8. **مراجعة بائعينك**

إنك مسؤول عن بائعينك بموجب اللائحة العامة لحماية البيانات. تطبيق الأحكام التعاقدية السليمة هام لكنه غير كاف. يجب أن تكون مطمئنًا إلى أن بائعينك يستوفون شروط اللائحة العامة لحماية البيانات ويمكنهم دعمك على صعيد التزامك باللائحة. سلهم كيف ينفذون اللائحة العامة لحماية البيانات

9. **مواكبة المستجدات القانونية/التنظيمية (المادة 29 المبادئ التوجيهية لمجموعة العمل، الدول الأعضاء المنفذة للقوانين)**

الإلمام باللائحة العامة لحماية البيانات كاف، أليس كذلك؟ لا! في الوقت الذي تنطبق فيه اللائحة العامة لحماية البيانات مباشرةً، تنفذ جميع الدول الأعضاء بالاتحاد الأوروبي قوانين حماية البيانات الوطنية المكملة.

هذه القوانين لازمة لتنظيم المناطق التي للدول الأعضاء سلطة تشريعية بها (على سبيل المثال خصوصية بيانات الموظفين) أو حيث تسمح لهم اللائحة العامة لحماية البيانات بسن المزيد من التشريعات (على سبيل المثال، معايير لمسؤولي حماية البيانات وعمليات تقييم تأثير حماية البيانات). بالإضافة إلى ذلك، تنشر المادة 29 مجموعة العمل توجيهات هامة. متابعة المستجدات أمرٌ صعب لكنه هام.[13]

خطة BLACKBOARD ونهجها

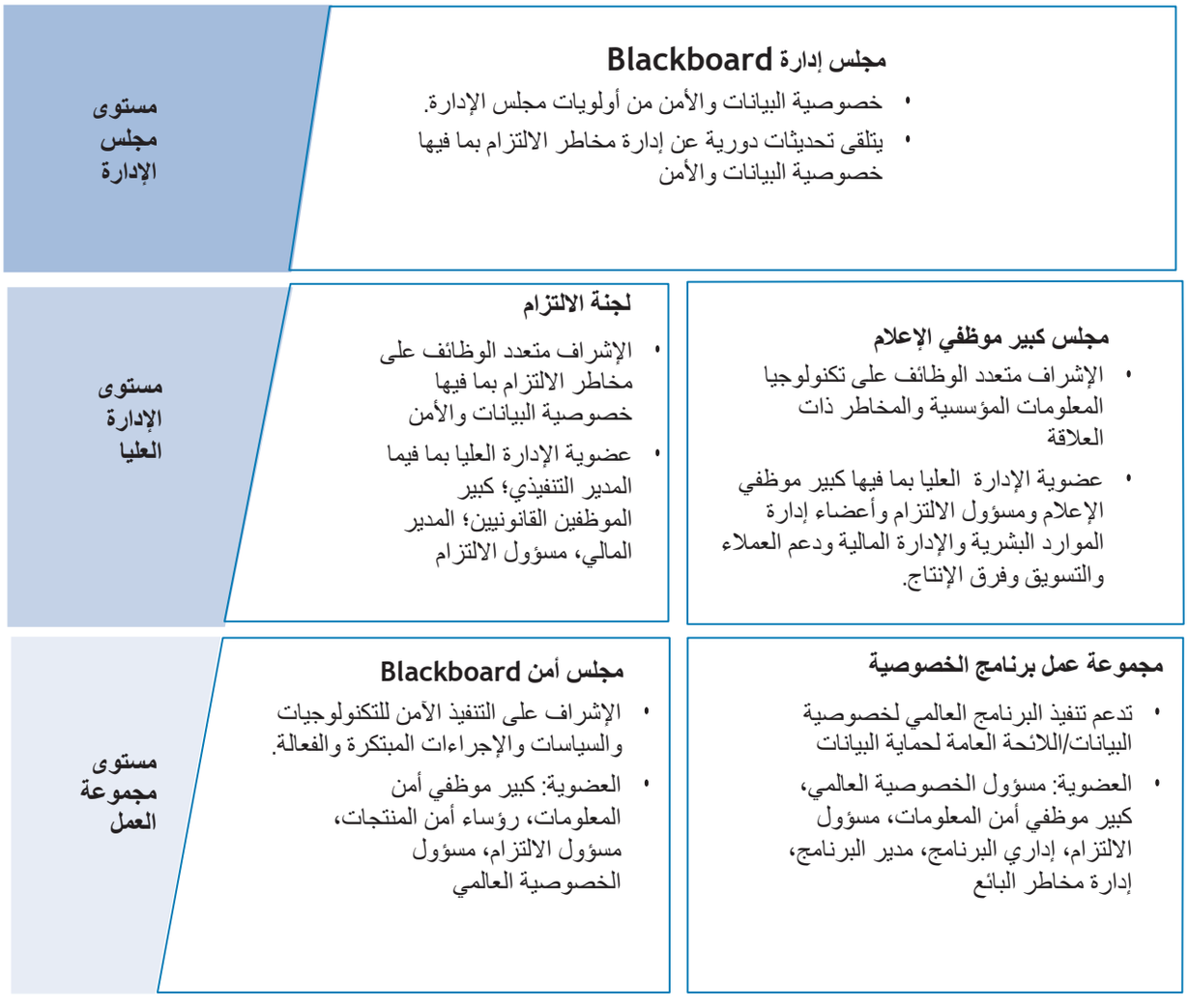
خصوصية البيانات والأمن في Blackboard

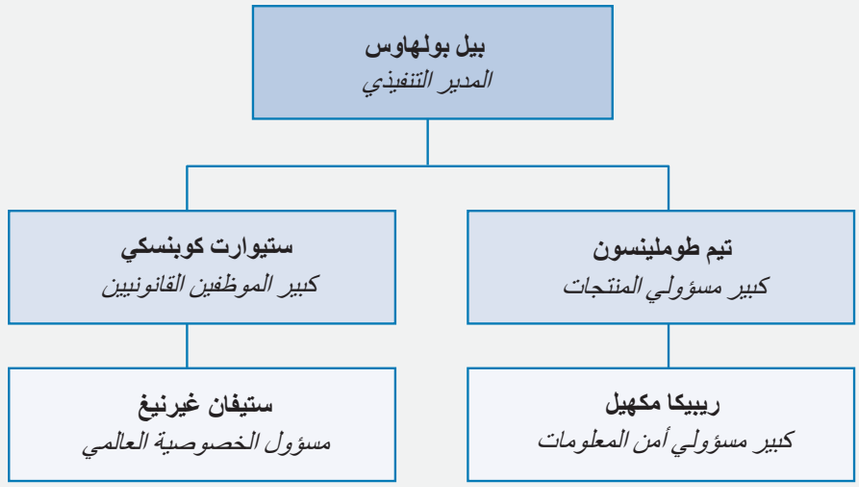
لطالما كانت خصوصية البيانات والأمن على رأس أولويات Blackboard. بالنسبة لنا، تعتبر اللائحة بمثابة فرصة لمزيد من التعزيز لممارساتنا القائمة الخاصة بخصوصية البيانات.

ولطالما كان نهجنا الخاص بخصوصية البيانات مركزًا على العميل. إننا نتفهم التحديات التي يواجهها عملاؤنا ولدينا الرغبة في مساعدتك.

تتطلب الممارسات الجيدة لخصوصية البيانات نموذج حوكمة قويًا. إن خصوصية البيانات والأمن في Blackboard واحدة من أولويات مجلس الإدارة ويضمن نموذج حوكمتنا (أنظر أدناه) إشراف الإدارة العليا ودعمها لما نبذله من جهود خصوصية البيانات والأمن.

كما تبرُز الأهمية التي تضعها Blackboard على خصوصية البيانات والأمن من خلال حقيقة أن مسؤول الخصوصية العالمي وكبير مسؤولي أمن المعلومات [14]يرفعون تقاريرهم إلى فريق القيادة التابع للمدير التنفيذي (انظر المخطط التنظيمي أدناه)





الخصوصية والأمن

تبرُز أيضًا الأهمية التي تضعها Blackboard على خصوصية البيانات وأمنها من خلال حقيقة أن مسؤول الخصوصية العالمي وكبير مسؤولي أمن المعلومات يرفعون تقاريرهم إلى فريق القيادة التابع للمدير التنفيذي.

نهج Blackboard الخاص باللائحة العامة لحماية البيانات

لقد أنشأنا مشروعًا شاملاً لتنفيذ شروط اللائحة العامة لحماية البيانات باستخدام النهج التالي:

- يبني تنفيذ اللائحة العامة لحماية البيانات على تجربة خصوصية البيانات القائمة وآليات الالتزام
- يتولى مسؤول الخصوصية العالمي قيادة تنفيذ اللائحة العامة لحماية البيانات بدعمٍ من مدير مشروع مخصص و"خبراء في اللائحة العامة لحماية البيانات" في كل مجال وظيفي
- وقد شاركت شركة المحاماة المعروفة، Bristows LLP، من بين آخرين، في جعم تنفيذ اللائحة العامة لحماية البيانات
- تشرف لجنة الالتزام بـ Blackboard على تنفيذ اللائحة العامة لحماية البيانات وتضم هذه اللجنة المدير التنفيذي للشركة وكبير الموظفين القانونيين وغيرهم من كبار المسؤولين

اللائحة العامة لحماية البيانات كفرصة

إننا لا ننظر إلى تنفيذ اللائحة العامة لحماية البيانات كمجرد جهد للالتزام بالشروط الأوروبية الجديدة لخصوصية البيانات فحسب، ولكن أيضًا كفرصة. على هذا النحو، نهدف إلى استغلال تنفيذ اللائحة العامة لحماية البيانات لإنجاز ما يلي:

- تعزيز الممارسات العالمية لخصوصية البيانات – سنستغل مشروع اللائحة العامة لحماية البيانات في تعزيز برنامجنا العالمي لخصوصية البيانات داخل الاتحاد الأوروبي وخارجه
- تطوير عمليات الخصوصية حسب التصميم التي تزيد من إدماج التزام خصوصية البيانات في عملياتنا اليومية
- دعم عملائنا في ما يبذلونه من جهود للالتزام باللائحة العامة لحماية البيانات
- تنصيب Blackboard كشركة خصوصية البيانات الرائدة المعترف بها في تكنولوجيا التعليم

خطة تنفيذنا

إننا نتبع منهجية Bristow LLP ثلاثية المراحل المعترف بها لتنفيذ البرنامج العالمي لخصوصية البيانات/برنامج اللائحة العامة لحماية البيانات. تستخدم هذه المنهجية للعديد من الشركات الأخرى بما فيها شركات التكنولوجيا الرائدة. فيما يلي المراحل الثلاثة الرئيسية:

- **المرحلة الأولى - جمع المعلومات**
- **المرحلة الثانية - تطوير الحلول**
- **المرحلة الثالثة - مسارات عمل التنفيذ**

لقد استخدمنا هذه المنهجية ثلاثية المراحل في تطوير برنامجنا مع المراحل الرئيسية الأربعة التالية:

بدء المشروع

شملت مرحلة بدء المشروع الأنشطة التالية:

- إحاطة الإدارة العليا وإشراكها
- تعيين مسؤول خصوصية عالمي يتولى مسؤولية قيادة مشروع اللائحة العامة لحماية البيانات
- تطوير خطة وحوكمة المشروع
- الجمع الأولي للمعلومات وتقييم أنشطة الالتزام الحالية للمناطق التي تتطلب تحسينات بموجب اللائحة العامة لحماية البيانات

المرحلة الأولى - جمع المعلومات (ورش العمل)

خلال المرحلة الأولية، أجرينا محادثات/ ورش عمل منظمة مع أصحاب المصلحة الرئيسيين من المناطق الوظيفية ومجموعات المنتجات في Blackboard للحصول على معلومات تفصيلية عن ممارسات معالجة البيانات في إطار تلك المناطق.

استخدمت مخرجات ورش العمل في إجراء تجليل للفجوات وتطوير الحلول وتنفيذ الخطط في المرحلة الثانية.

المرحلة الثانية - تطوير الحلول

بناءً على المعلومات المستمدة من ورش العمل، طورنا الحلول والوثائق التالية:

- التوثيق المحسن لخصوصية البيانات الداخلية (السياسة ومعايير التشغيل التفصيلية) الذي يعكس شروط اللائحة العامة لحماية البيانات ويوضح كيفية وجوب استيفاء شروط اللائحة العامة لحماية البيانات لمختلف أنشطة معالجة البيانات (على سبيل المثال شروط معالجة بيانات العملاء، وعملية الخصوصية حسب التصميم)
- شروط المنتجات
- خطط تنفيذ للمناطق الوظيفية وللجهود المطلوبة مركزيًا

المرحلة الثالثة - مسارات عمل التنفيذ

خلال المرحلة النهائية، ننفذ التوثيق المتطور لخصوصية البيانات وننفذ خطط التنفيذ. ستستخدم ستة مسارات عمل رئيسية لإنجاز التنفيذ:

1. تنفيذ خطط التنفيذ للمناطق الوظيفية ومجموعات المنتجات
2. مراجعة السياسات والإشعارات والموافقات العامة وتحديثها
3. تعزيز الحوكمة (الأدوار والمسؤوليات، التدريب، الخصوصية حسب التصميم، إلخ)
4. مراجعة وتحديث عقود البائعين (عند الضرورة)[15]
5. تغييرات أنظمة تكنولوجيا المعلومات (عند الضرورة)
6. إنشاء سجل لمعالجة البيانات

نبذة عن التغييرات

يوضح الجدول أدناه كيفية تصورنا للحالة النهائية برنامجنا الخاص باللائحة العامة لحماية البيانات/ خصوصية البيانات عقب أنشطة التنفيذ. بعد تنفيذ اللائحة العامة لحماية البيانات، سنواصل الابتكار والتكيف لمزيد من النضج لممارساتنا الخاصة بخصوصية البيانات.

كيف سيساعدك برنامجنا الخاص باللائحة العامة لحماية البيانات؟

يركز برنامج Blackboard العالمي لخصوصية البيانات/لتنفيذ اللائحة العامة لحماية البيانات على دعم مؤسستك في تنفيذك للائحة العامة لحماية البيانات. ستوفر الأقسام التالية مزيدًا من التفاصيل ولكن النقاط السبعة الرئيسية بإيجاز هي:

1. **المنتجات الجاهزة لاستيفاء شروط اللائحة العامة لحماية البيانات:** إننا ننفذ شروط المنتجات لدعم العملاء في شروط الشفافية وطلبات الحقوق الفردية، إلخ.
2. **الخصوصية حسب التصميم:** إننا ننفذ مفهوم الخصوصية حسب التصميم وعملية تقييم تأثير حماية البيانات لتسهيل توثيق الالتزام
3. **عمليات نقل البيانات:** سنواصل نهجنا متعدد الطبقات: الإقليمية ودرع الخصوصية الأوروبي الأمريكي والشروط النموذجية المعتمدة من الاتحاد الأوروبي
4. **العقود مع العملاء:** لدينا ملحق خاص بمعالجة البيانات الجاهزة لاستيفاء شروط اللائحة العامة لحماية البيانات لاتفاقيتنا الرئيسية القياسية
5. **بائعونا:** لدينا عقود قوية وإطار عمل لإدارة مخاطر البائعين مطبق
6. **الأمن:** لقد وضعنا السياسة والإجراءات والحوكمة التي تعزز باستمرار لضمان أمن بيانات العملاء
7. **إشعار الخرق:** لدينا عملية موثقة ومختبرة لمواجهة الحوادث الأمنية

1. المنتجات الجاهزة لاستيفاء شروط اللائحة العامة لحماية البيانات

دعم عملائنا بجعل منتجاتنا جاهزة لاستيفاء شروط اللائحة العامة لحماية البيانات هو أحد أهم جوانب مسارات عملنا الخاصة بتنفيذ هذه اللائحة. لهذا الغرض، وضعنا الحد الأدنى من شروط اللائحة العامة لحماية البيانات/خصوصية البيانات لمنتجاتنا. تمشيًا مع منهجنا الرامي إلى تعزيز ممارساتنا الخاصة بخصوصية البيانات عالميًا، تنطبق معظم هذه الشروط على جميع منتجاتنا وليس فقط المنتجات التي نوفرها داخل الاتحاد الأوروبي. يدعم ذلك أيضًا عملاءنا خارج الاتحاد الأوروبي التي تقع ضمن نطاق اللائحة العامة لحماية البيانات.

طورنا شروطنا الخاصة باللائحة العامة لحماية البيانات/منتجات خصوصية البيانات من خلال عملية قوية ومكثفة. وقمنا بصياغة نسخة أولية بالاستعانة بمستشار خارجي. خلال جلسات العمل المتعددة والمراجعات مع أصحاب المصلحة الرئيسيين من فرقنا لتطوير المنتجات وإدارتها، قمنا بتنقيح النسخة في صورة شروط عامة محددة وعملية للمنتجات مصحوبة بإرشادات تفصيلية. ثم تُرجمت هذه الشروط الخاصة باللائحة العامة لحماية البيانات/منتجات خصوصية البيانات إلى إجراءات خاصة بالمنتجات في خطط تنفيذ المنتجات لكل مجموعة منتجات.

يمكن تصنيف شروط [16] منتجاتنا على النحو التالي:

الشفافية

- قدرة العملاء على الربط بسياساتهم/إشعاراتهم الخاصة بالخصوصية
- توفير معلومات عن كيفية استخدام المعلومات الشخصية عمومًا في أي منتج

تقليل/ حذف البيانات

- مراجعة المنتجات للمجالات غير الضرورية/الاختيارية
- مراجعة المنتجات لتوفير فرص لاستخدام بيانات مستعارة أو مجهولة الهوية بدلاً من المعلومات الشخصية
- القدرة على حذف المعلومات الشخصية عند طلب العملاء ذلك (في الحالات التي لا يمكن للعملاء/المستخدمين فيها حذف البيانات بأنفسهم)

حقوق الأفراد العامة

- القدرة على توفير الوصول إلى المعلومات الشخصية وتصحيحها عند طلب الفرد ذلك
- القدرة على حذف المعلومات الشخصية عند طلب الفرد ذلك

حقوق الأفراد داخل الاتحاد الأوروبي

- القدرة على التعامل مع طلبات نقل البيانات (حق الأفراد في استقبال البيانات بصيغة مقروءة آليًا في ظروفٍ معينة)
- القدرة على التوقف عن استخدام المعلومات الشخصية (حق الاعتراض/ حق فرض القيود في ظروف معينة)

لقد وضع Blackboard بالفعل برامج لأمن منتجاتنا تأخذ اللائحة العامة لحماية البيانات بعين الاعتبار. لذلك لم نحدد أي شروط إضافية لأمن المنتجات في ضوء اللائحة العامة لحماية البيانات.[17]

2. الخصوصية حسب التصميم

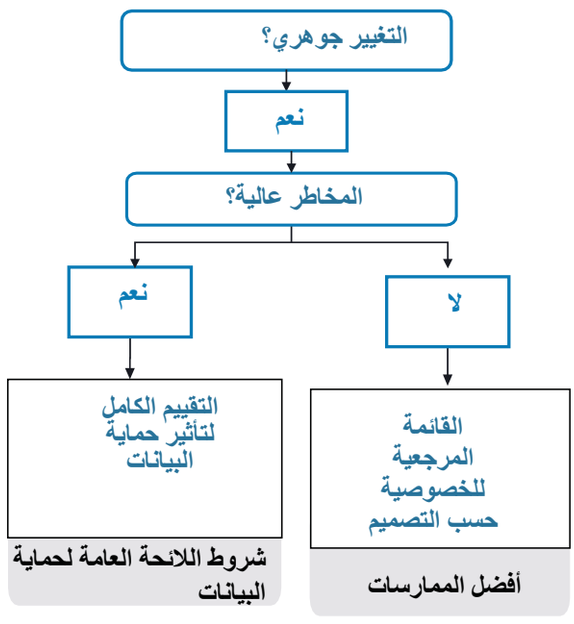
نظرًا أنه بات من الصعب بشكل أكبر في عالم اليوم على الأفراد أن يظلوا متحكمين في معلوماتهم (انظر منشورنا على مدونة الخصوصية اليومية عن هذا الموضوع)، أصبحت الخصوصية حسب التصميم والمساءلة ذات أهمية متزايدة للحفاظ على ثقة الأفراد والعملاء والمنظمين ولتوثيق كيفية التزام أي مؤسسة باللائحة العامة لحماية البيانات. ولذلك نضع نهج الخصوصية حسب التصميم في قلب برنامجنا العالمي لخصوصية البيانات/ للائحة العامة لحماية البيانات.

بالنسبة لـ Blackboard، يعد ذلك تطورًا لا ثورة. لقد أجرينا دائمًا مراجعات قانونية للمنتجات والممارسات الجديدة.
ومن خلال نهج الخصوصية حسب التصميم خاصتنا فإننا نضفي الطابع الرسمي على هذه المراجعات ونوثقها توثيقًا أفضل.

النهج

- لقد أنشأنا عملية وقائمة مرجعية موثقة للخصوصية حسب التصميم.
- تُدرج المناطق الوظيفية ومجموعات المنتجات القائمة المرجعية للخصوصية حسب التصميم في عمليات تغييرها.
- يتطلب كل تغيير جوهري في كيفية استخدام المعلومات الشخصية الانتهاء من القائمة المرجعية للخصوصية حسب التصميم. وفي حين أن اللائحة العامة لحماية البيانات لا تقتضي ذلك على وجه التحديد، فإن ذلك يُعد أفضل الممارسات.
- ستطلق القائمة المرجعية تقييمًا أكثر تفضيلاً لتأثير حماية البيانات للاستخدام عالي المخاطر للمعلومات الشخصية (شرط للائحة العامة لحماية البيانات)

يوضح الرسم البياني التالي النهج:



3. عمليات نقل البيانات

لا تدخل اللائحة العامة لحماية البيانات أي تغييرات جوهرية على كيفية نقل المعلومات الشخصية خارج الاتحاد الأوروبي/المنطقة الاقتصادية الأوروبية. تظل القيود الحالية وآليات نقل البيانات. يعني ذلك السماح بعمليات نقل البيانات في حالة تطبيق آلية أوروبية معتمدة لنقل البيانات كدرع الخصوصية الأوروبي الأمريكي أو الشروط النموذجية المعتمدة من الاتحاد الأوروبي (اتفاقيات نقل البيانات). تضمن هذه الآليات حماية المعلومات الشخصية كما يجب حتى عند مغادرة الاتحاد الأوروبي/المنطقة الاقتصادية الأوروبية.

سنواصل نهجنا متعدد الطبقات والمسهب للالتزام بنقل البيانات. يعني ذلك أننا نتعامل مع شروط نقل البيانات بطرقٍ متعددة لضمان توفير الحماية الواجبة لمعلوماتك.

- **الاستضافة الإقليمية:** لدينا استراتيجية استضافة إقليمية مع استضافة جميع المنتجات تقريبًا في الاتحاد الأوروبي والتخطيط لنقل المنتجات الأخرى لحلول الاستضافة الإقليمية. في حين أن اللائحة العامة لحماية البيانات لا تقتضي التخزين الإقليمي وأننا لا نعتقد بأن توطين البيانات من شأنه أن يؤدي إلى خصوصية أو أمن أفضل للبيانات،[18] فإننا نتفهم أن العديد من عملاء الاتحاد الأوروبي يفضلون أن تخزن بياناتهم في الاتحاد الأوروبي.
- **درع الخصوصية:** Blackboard هو درع خصوصية أوروبي أمريكي معتمد يسمح لنا بنقل البيانات الشخصية بشكل قانوني للولايات المتحدة.
- **الشروط النموذجية:** كما نستخدم اتفاقيات "الشروط النموذجية" المعتمدة من الاتحاد الأوروبي التي تسمح لنا بنقل البيانات الشخصية وفقًا للشروط خارج المنطقة الاقتصادية الأوروبية داخل مجموعة شركات Blackboard("اتفاقية نقل بيانات العملاء").
- **بائعونا:** هناك عقود صارمة مبرمة مع البائعين والشركاء (كشركة آي بي إم؛ أمازون ويب سيرفسيز) لضمان نقل شروط نقل البيانات (وغيرها من التزامات حماية البيانات) إلى بائعينا وشركائنا.

لدينا في الوقت الراهن[19] العديد من مراكز البيانات الإقليمية لدعم معالجة البيانات في الاتحاد الأوروبي لعملائنا من دول الاتحاد الأوروبي:

- الاستضافة المدارة (مراكز بيانات Blackboard): مراكز البيانات في أمستردام (هولندا) وفرانكفورت (ألمانيا).
- الاستضافة السحابية (مركز بيانات أمازون ويب سيرفسيز): منطقة أمازون ويب سيرفسيز فرانكفورت، ألمانيا (مركز الاتحاد الأوروبي).

تستوفي مراكز بيانات أمازون ويب سيرفسيز مجموعة من الاعتمادات والشروط من الأيزو 27001 و27018 إلى SOC2 والالتزام باللائحة العامة لحماية البيانات وكذلك الالتزام بالشروط المحلية مثل C5 الألمانية و-IT Grundschutz.[20]

من المهم أن نفهم أنه بينما يتم تخزين المعلومات الشخصية للعملاء في مراكز البيانات المذكورة فيما يتعلق بمعظم المنتجات (بما في ذلك ليرن 9.1 وليرن ساس ومودلرومزوكولابورايت) للعملاء من دول الاتحاد الأوروبي، قد تكون هناك حاجة إلى الوصول إلى هذه البيانات من خارج الاتحاد الاوروبي/المنطقة الاقتصادية الأوروبية لتقديم المنتجات والخدمات، على سبيل المثال الدعم على مدار الساعة. يُسمح بعمليات نقل البيانات المذكورة بفضل اعتماد درع الخصوصية الأوروبي الأمريكي والشروط النموذجية المذكورة.

4. العقود مع العملاء

يقتضي التوجيه الحالي مراقب بيانات لإبرام عقد مع البائع (معالج البيانات)، ولكن لا يصف محتوى العقد بالتفصيل. اللائحة العامة لحماية البيانات وصفية أكثر وتتضمن قائمة بالمحتوى المطلوب.[21]

يتضمن ملحقنا الحالي القياسي لمعالجة البيانات جميع النقاط المطلوبة أدناه. يتم تضمينها تلقائيًا للعملاء في اتفاقيتنا الرئيسية القياسية الواقعين ضمن نطاق اللائحة العامة لحماية البيانات.

- ✓ استخدم البيانات الشخصية فقط وفقًا للتعليمات
- ✓ يجب على العاملين التوقيع على اتفاقيات السرية
- ✓ يجب اتخاذ التدابير الأمنية الواجبة
- ✓ أشرك البائعين فقط (المعالجون الثانويون) ...
  - على النحو المصرح به من جانب مراقب البيانات (يمكن أن يكون تصريح عام)
  - المطلوبة تعاقديًا لاستيفاء التزامات حماية البيانات ذاتها
- ✓ ساعد المراقب في الرد على طلبات الحقوق الفردية
- ✓ ساعد المراقب في التدابير الأمنية وإشعار خرق حماية البيانات وحماية البيانات عمليات تقييم التاثير
- ✓ إعادة البيانات أو حذفها في نهاية العقد
- ✓ قدم المعلومات اللازمة لمراقب البيانات لإثبات الالتزام
- ✓ أبلغ مراقب البيانات على الفور إذا ما كان هناك أي تعليمات من جانبه تخرق اللائحة العامة لحماية البيانات

5. إدارة بائعينا

تستعين Blackboard ببائعين (مثل آي بي إم، أمازون ويب سيرفسيز) لمساعدتنا في تقديم منتجاتنا وخدماتنا لعملائنا. بينما يتطلب ذلك الوصول إلى المعلومات الشخصية لعملائنا، تتحمل Blackboard مسؤولية ممارسات خصوصية البيانات الخاصة بالبائعين.

كجزء من برنامجنا الخاص باللائحة العامة لحماية البيانات، فإننا نربط بشكل وثيق نهج الخصوصية حسب التصميم بالعمليات القائمة لإدارة مخاطر البائعين والشراء. يترتب على ذلك الضوابط الرئيسية التالية:

- عقود صارمة مصحوبة بملحق للخصوصية وللائحة العامة لحماية البيانات مبرمة مع أطراف ثالثة تفرض شروطًا متكافئة بدرجة كبيرة نطبقها مع عملائنا
- اتفاقيات "الشروط النموذجية" و/أو ملحق اللائحة العامة لحماية البيانات ودرع الخصوصية لتمكين عمليات نقل البيانات المشروعة إلى بائعينا
- سياسة وإطار عمل موثقان لإدارة مخاطر البائعين
- يجب على البائعين الجدد الذين بإمكانهم الوصول إلى المعلومات الشخصية إكمال استبيان تقييم أمن البائعين المتضمن لأسئلة عن الالتزام بخصوصية البيانات
- يجب على البائعين الذين بإمكانهم الوصول إلى أنظمة Blackboard المدارة اتباع سياسات Blackboard لرقابة الوصول الداخلية والهوية والترخيص ولتضمين مراجعات الحسابات كما يجب
- يجب على البائعين الوصول إلى موارد Blackboard من خلال الآليات المعتمدة (مثل الشبكة الخاصة الافتراضية VPN)
- يجب أن يمتلك البائعون ضوابط وصول محدودة على الحركة والمستخدمين والأصول

6. الأمن

لا تغير اللائحة العامة لحماية البيانات التدابير الفنية والتشغيلية تغييرًا جوهريًا للحفاظ على أمن المعلومات الشخصية. يجب أن تكون هذه التدابير "مناسبة" للمخاطر المتضمنة في التوجيه الحالي. ولذلك، فإننا نواصل الاعتماد على برامجنا المطبقة لأمن المعلومات.

تنظيم مخاطر أمن المعلومات

لقد وضعنا السياسة والإجراءات والحوكمة والشروط الفنية لإدارة مخاطر أمن تكنولوجيا المعلومات على مستوى الأعمال التجارية.

ومن اليوم الأول، يجب على العاملين في Blackboard تفهم مسؤوليتهم لحماية البيانات الشخصية للعملاء.

- الإقرار بالسياسة لحماية المعلومات الحساسة
- التدريب السنوي لأمن المستخدم وخصوصية البيانات
- تمارين التصيد الاحتيالي
- نشرات التوعية

الشروط التالية مطبقة لحماية البيانات عن طريق موظفينا:

- تحدد تصنيفات البيانات مع شروط حماية كل نوع من أنواع البيانات. بيانات عملائنا هي الأعلى حساسيةً - بيانات المؤسسات التعليمية والدارسين بها.
- الضوابط الفنية مطبقة لحماية البيانات، على سبيل المثال:
  - استخدام التشفير
  - التحديثات الأمنية العاجلة
  - ضوابط المصادقة المحسنة
  - الحماية من البريد الإلكتروني وحركة الويب الضارة
  - تقنيات حماية نقاط النهاية
  - الوصول المقيد على أساس الحاجة إلى المعرفة

الأمر لا يقتصر فقط على اللائحة العامة لحماية البيانات ...

كشركة عالمية، تخدم المجتمع التعليمي، نراقب عن كثب القوانين واللوائح ذات الصلة الخاصة بخصوصية البيانات والأمن الجغرافية والخاصة بقطاع التعليم.

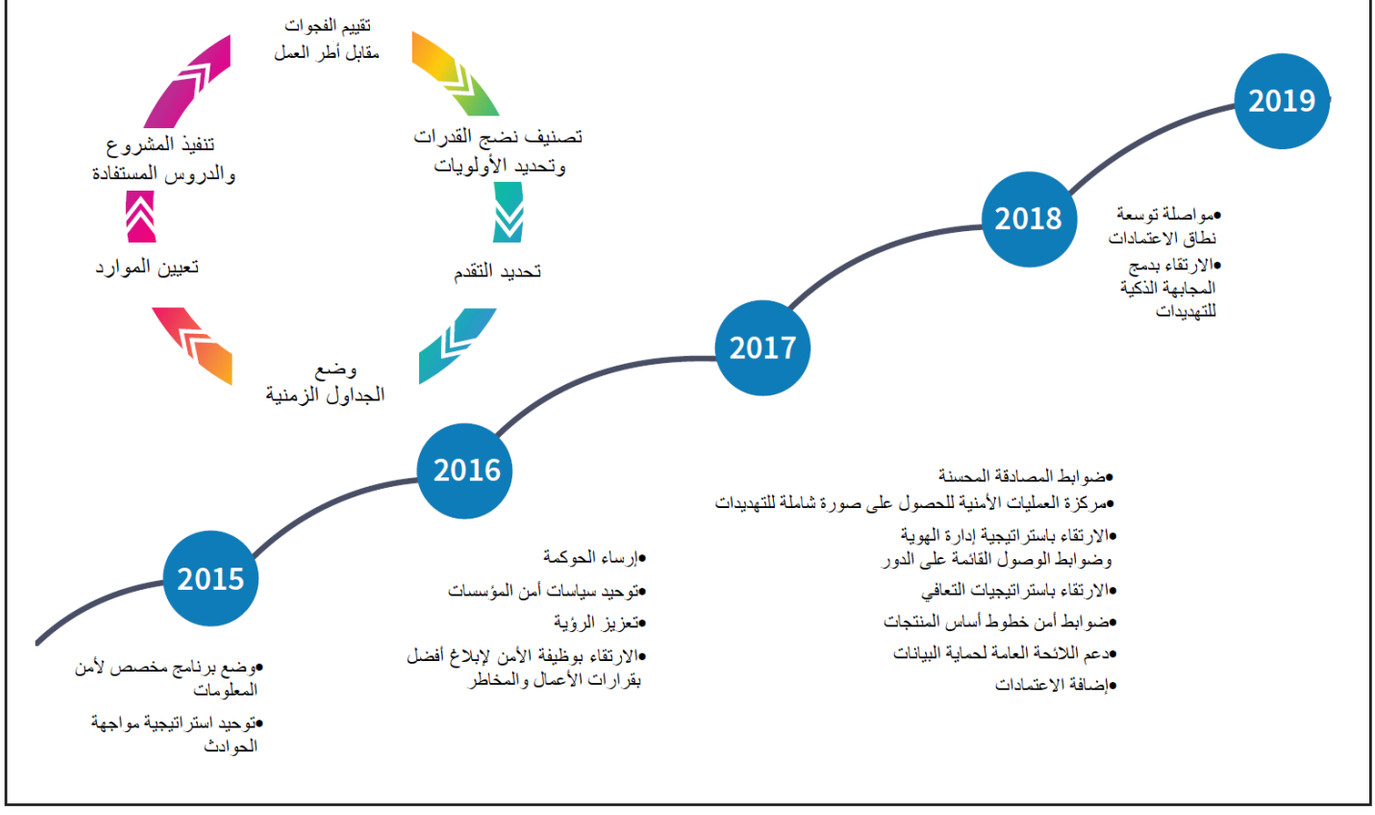
القائمة التالية مجرد بعض الأمثلة على لوائح الأمن وخصوصية البيانات.
المعايير وأطر العمل التي تأخذها Blackboard بعين الاعتبار بالإضافة إلى اللائحة العامة لحماية البيانات عند وضع سياسات الأمن والعمليات والضوابط الفنية الخاصة بنا.

- القانون الأمريكي للخصوصية والحقوق التعليمية للأسرة وتعديل حماية حقوق التلاميذ
- القانون الأمريكي لحماية خصوصية الأطفال على الإنترنت
- قوانين الولايات الأمريكية (مزيج من القوانين القائمة والجديدة للولايات الخمسين)
- معايير الحكومة الأمريكية - برنامج إدارة المخاطر والتراخيص الفيدرالي
- معايير أمن بيانات صناعة بطاقات الدفع عند الضرورة
- الأيزو/اللجنة الكهروتقنية الدولية، أواسب، نست
- المعايير الدولية (متكس، إراب)

عمليات تقييم النضج الأمني وخرائط الطريق

نعمل جاهدين للاستمرار في تعزيز تدابير الأمنية الفنية والتشغيلية.
يوضح المخطط الموجود في الصفحة التالية عملياتنا المستمرة لتقييم النضج وخرائط طريقنا.

اعتماد أطر العمل: عمليات تقييم النضج الأمني وخرائط الطريق



7. إشعار الخرق

يعتبر الإشعار الإلزامي الجديد بخروقات البيانات الشخصية لسلطة حماية البيانات المختصة و (في بعض الحالات) الأفراد المتضررين، أحد التغييرات الرئيسية للائحة العامة لحماية البيانات.[22]

بالنسبة لمعظم منتجاتنا وخدماتنا، Blackboard معالج بيانات[23]في ضوء اللائحة العامة لحماية البيانات. لذلك يتحمل عملاؤنا التزام إبلاغ سلطات حماية البيانات والأفراد في حالة خرق يشمل Blackboard. إلا أن اللائحة العامة لحماية البيانات تشترط على معالجي البيانات مثل Blackboard إبلاغ عملائهم (مراقبي البيانات) دون تأخير غير مبرر (أي "على الفور")[24] في مثل هذه الحالة.

إننا نطبق التدابير التالية التي تساعد عملائنا في الوفاء بالتزاماتهم في حالة خرق البيانات الشخصية في Blackboard وذلك فيما يتعلق بأي عميل:

- عملية Blackboard لمواجهة الحوادث الأمنية
  - موثقة ومختبرة بانتظام
  - تسهل التحديد والتحقيق والعلاج السريع في حالة وقوع أي حادث
  - تسمح بالإشعارات الفورية للعملاء
  - تعتمد على الفريق المكرس لمواجهة الحوادث الأمنية (الذي يشمل كبير مسؤولي أمن المعلومات ومسؤول الخصوصية العالمي)
- ورد ذكر التزامنا بإشعار العملاء على الفور صراحةً في اتفاقيتنا الرئيسية القياسية الحالية وملحق حماية البيانات[25]

الخاتمة

تتطلب اللائحة العامة لحماية البيانات تغييرات جوهرية يتجاوز تأثيرها تاريخ الالتزام في 25 مايو 2018. نأمل أن تساهم هذه الورقة البيضاء في نجاح تنفيذك للائحة العامة لحماية البيانات وأن تكون قد أوضَحَت مدى تعامل Blackboard بجدية مع اللائحة العامة لحماية البيانات والتزام خصوصية البيانات.

توفر الأقسام التالية المزيد من المعلومات المفيدة وتتضمن البريد الإلكتروني المخصص للتواصل معنا لأي استفسارات أو ملاحظات على هذه الورقة.

الموارد المفيدة للائحة العامة لحماية البيانات

الموارد المرتبطة أدناه مجرد مجموعة صغيرة من المواد المفيدة المتاحة عبر الإنترنت. لا يُقصد منها أن تكون قائمة شاملة.

برجاء استشارة المتخصصين لمزيد من التحليل التفصيلي لكيفية انطباق اللائحة العامة لحماية البيانات عليك. من المهم الاعتماد على خبراء في حماية البيانات (على سبيل المثال من إحدى شركات المحاماة التي تختارها).

الموارد الرسمية للاتحاد الأوروبي

- نص اللائحة العامة لحماية البيانات
- المادة 29 المبادئ التوجيهية لمجموعة العمل
- الموقع الإلكتروني للائحة العامة لحماية البيانات التابع للمفوضية الأوروبية

مواد هيئة حماية البيانات بالاتحاد الأوروبي

- يوجد لمكتب المفوض الإعلامي بالمملكة المتحدة موقع إلكتروني ممتاز عن اللائحة العامة لحماية البيانات يتضمن مواد مفيدة بلغة مبسطة يتم تحديثها باستمرار
- يوجد لمفوض حماية البيانات الأيرلندي صفحة مخصصة للائحة العامة لحماية البيانات للمؤسسات
- توفر هيئة حماية البيانات الفرنسية بعض الموادباللغة الإنجليزية بما في ذلك برنامج مجاني لتقييم تأثير الخصوصية (والمزيد من المواد باللغة الفرنسية)
- أصدرت وكالة حماية البيانات الإسبانية دليلاً للمؤسسات التعليمية (بصيغة بي دي إف بالإسبانية)

دليل شركات المحاماة

- دليل Bird & Bird للائحة العامة لحماية البيانات
- متعقب قوانين الدول الأعضاء الصادر عن Bird & Bird (تعقب التغيرات الوطنية في اللائحة العامة لحماية البيانات)
- دليل النجاة الخاص باللائحة العامة لحماية البيانات الصادر عن لينكليترز (بي دي إف)
- دليل اللائحة العامة لحماية البيانات الصادر عن White & Case

المؤسسات الأخرى

- تمتلك مؤسسة جيه آي إس سي المملكة المتحدة موارد مفيدة وأحداث وتحديثات مدونات للائحة العامة لحماية البيانات
- نشرت مؤسسة UCISA وثيقة لأفضل ممارسات اللائحة العامة لحماية البيانات تتضمن خطوات عملية و دراسات حالة
- تمتلك الرابطة الدولية لمتخصصي الخصوصية نشرة إخبارية أسبوعية جيدة (مجانية) عن تطورات خصوصية البيانات الأوروبية
- كما تمتلك الرابطة نبذة مفيدة عن مقدمي أدوات خصوصية البيانات (بي دي إف)
- تمتلك أمازون ويب سيرفسيز مركزًا مخصصًا للائحة العامة لحماية البيانات

السير الذاتية

ستيفان غيرنيغ
مسؤول الخصوصية العالمي

- يتحمل المسؤولية العالمية عن الالتزام بقوانين خصوصية البيانات والأمن
- يدير البرنامج العالمي لخصوصية البيانات/تنفيذ اللائحة العامة لحماية البيانات
- يرفع التقارير إلى كبير الموظفين القانونيين؛ عضو الفريق القانوني في Blackboard
- مقيم في لندن

معلومات أساسية عن ستيفان:

- محامي/ نائب مفوض حماية البيانات في الهيئة السويسرية لحماية بيانات المقاطعات (2002-2008)
- ماجستير في القانون من كلية لندن الجامعية (2008-2009)
- مديرمساعد، خصوصية المجموعة في باركليز (2010-2012)
- المدير الإقليمي لعمليات خصوصية البيانات في منطقة أوروبا والشرق الأوسط وأفريقيا بسيتي جروب (2012-2014)
- كبير مسؤولي الخصوصية في منطقة أوروبا والشرق الأوسط وأفريقيا ومنطقة آسيا والمحيط الهادئ بسيتي جروب (2014-2017)
- خبير معتمد في خصوصية البيانات في أوروبا بموجب CIPP/E

ريبيكا مكهيل
كبير مسؤولي أمن المعلومات

- تدير استراتيجية أمن المنتجات والبنية الأساسية
- تشرف على حوكمة الأمن السيبراني لـ Blackboard
- ترفع التقارير لكبير مسؤولي المنتجات
- مقيمة في واشنطن العاصمة

معلومات أساسية عن ريبيكا:

- التحقت بالعمل في Blackboard في عام 2016؛ قامت مؤخرًا بتوحيد الفرق الأمنية وارتقت بدور المنظومة الأمنية بالشركة
- ماجستير في الرياضيات المتقطعة وتطبيقات الحوسبة في رويال هولواي، جامعة لندن
- مدير أول سابق للبرامج الإلكترونية في شركة نوفيتا وشركة سسرا التي تقدم الخدمات للحكومة الأمريكية والعملاء التجاريين - على سبيل المثال، وزارة الخارجية وإدارة أمن النقل والمؤسسة الفيدرالية للتأمين على الودائع

المزيد من المعلومات

يمكنك الاطلاع على مزيد من المعلومات على صفحتنا المخصصة لخصوصية البيانات والمجتمع الأمني.

كما نمتلك نشرة إخبارية عن خصوصية البيانات. إذا كنت ترغب في تلقي نشرتنا الإخبارية أو إذا كانت لديك أي استفسارات أو ملاحظات على هذه الورقة البيضاء، برجاء الاتصال بنا على privacy@blackboard.com.

المصادر

1 انظر قسم " الموارد المفيدة للائحة العامة لحماية البيانات" في النهاية لمزيد من الإرشادات التفصيلية عن اللائحة العامة لحماية البيانات.

2 إننا نفضل استخدام تعبير "المعلومات الشخصية" عن "البيانات الشخصية" ولكن نستخدمه بنفس المعنى والنطاق الخاص "بالبيانات الشخصية"

3 مراقب البيانات هو المؤسسة التي تحدد وسائل معالجة البيانات وأغراضها (كيفية استخدام المعلومات الشخصية والغرض منه).

4 انظر قسم "دورنا ودور مؤسستك بموجب اللائحة العامة لحماية البيانات.

5 انظر قسم "تبسيط اللائحة العامة لحماية البيانات" أدناه لمزيد من التفاصيل عن عمليات نقل البيانات.

6 انظر "مقدمة عن مشروع قانون حماية البيانات" الصادرة عن مكتب المفوض الإعلامي بالمملكة المتحدة" للاطلاع على نبذة مفيدة عن مشروع القانون.

7 انظر أيضًا منشورات مدونة المكتب عن خرافات اللائحة العامة لحماية البيانات.

8 انظر أيضًا المبادئ التوجيهية للمادة 29 مجموعة العمل (مسودة) بشأن الموافقة بموجب اللائحة 679/2016 (المادة 259 مجموعة العمل) وإرشادات مكتب المفوض الإعلامي بالمملكة المتحدة الخاصة بالموافقة.

9 المبادئ التوجيهية للمادة 29 مجموعة العمل بشأن إشعار خرق البيانات الشخصية بموجب اللائحة 679/2016 (المادة 250 مجموعة العمل، نسخة رقم .01).

10 انظر أيضًا قسم "عمليات نقل البيانات".

11 انظر على سبيل المثال إعداد مكتب المفوض الإعلامي بالمملكة المتحدة للائحة العامة لحماية البيانات -12 خطوة من الواجب اتخاذها الآن (بي دي إف).

12 انظر أيضًا قسم "تبسيط اللائحة العامة لحماية البيانات".

13 انظر أيضًا قسم "الموارد المفيدة للائحة العامة لحماية البيانات".

14 لمزيد من المعلومات عن كبير مسؤولي أمن المعلومات ومسؤول الخصوصية العالمي، انظر قسم السير الذاتية.

15 كجزء من مشروع اعتماد درع الخصوصية الأوروبي الأمريكي، أدرجنا بالفعل الأحكام التعاقدية الخاصة باللائحة العامة لحماية البيانات الضرورية في العديد من العقود المبرمة مع بائعينا (المعالجون الثانويون) الذين بإمكانهم الوصول إلى المعلومات الشخصية للاتحاد الأوروبي.

16 برجاء الملاحظة أن جميع شروط المنتجات لا تنطبق على جميع المنتجات. على سبيل المثال، بعض المنتجات غير مزودة بواجهة مستخدم تسمح للعملاء بالربط بسياسات/إشعارات الخصوصية خاصتهم.

17 انظر قسم "الأمن" لمزيد من التفاصيل.

18 عند توصيل شبكة أو نظام بالإنترنت، لا يكون للموقع المادي للبيانات أي تأثير يُذكر على التهديدات الأمنية. انظر الورقة البيضاء "إقامة البيانات، منظورات سياسة أمازون ويب سيرفسيز" (خاصةً الصفحتين 2 و3) الصادرة عن شركة أمازون ويب سيرفسيز Amazon Web Services للاطلاع على الحجج المقنعة الرافضة لتوطين البيانات.

19 اعتبارًا من تاريخ هذه الورقة.

20 انظر برامج الالتزام الخاصة بأمازون ويب سيرفسيز للاطلاع على القائمة الكاملة للاعتمادات والالتزام القانوني.

21 المادة 28(2)-(4)- من اللائحة العامة لحماية البيانات.

22 المادتان 33 و34 من اللائحة العامة لحماية البيانات.

23 للاطلاع على شرح دور معالج البيانات، انظر قسم "دورنا ودور مؤسستك بموجب اللائحة العامة لحماية البيانات".

24 انظر قسم "تبسيط اللائحة العامة لحماية البيانات" أعلاه لمزيد من التفاصيل عن توقيت وعملية الإشعار بخرق البيانات الشخصية

25 انظر أيضًا قسم "العقود مع العملاء".