Como a implementação do RGPD pela Blackboard auxilia nossos clientes

O Regulamento Geral sobre a Proteção de Dados da UE (RGPD) é uma mudança radical. A Blackboard saúda esta mudança. Nós nos preocupamos com a privacidade de dados e entendemos que é um direito humano. O RGPD reforça os direitos dos indivíduos e levará a melhores práticas de privacidade de dados. Isso beneficiará indivíduos e organizações, pois aumentará a confiança entre eles.

Estamos publicando este documento para proporcionar a nossos clientes uma visão geral das mudanças e dos mitos em torno do RGPD, explicar nossa abordagem de implementação e detalhar como nossos esforços apoiarão sua organização. Nós nos concentramos nas informações que achamos que serão mais úteis para você. Este artigo não é, portanto, um guia completo para o RGPD.[1]

O RGPD traz mudanças significativas, mas na Blackboard podemos nos construir sobre nossas práticas de privacidade de dados robustas já existentes (por exemplo, nossa certificação pelo Escudo de Proteção da Privacidade UE-EUA). Vemos o RGPD como uma oportunidade para fortalecer ainda mais nossas práticas. E continuaremos focados em nossos clientes e daremos suporte a você na conformidade com a privacidade de dados.

Estes materiais foram preparados apenas para fins informativos e não são aconselhamentos legais. Por favor, procure o aconselhamento de seus advogados internos ou externos na implementação do RGPD em sua organização e questões legais relacionadas.

ÍNDICE

RGPD - O QUE VOCÊ PRECISA SABER

A Blackboard é certificada pelo Escudo de Proteção da Privacidade, orgulhosa signatária do Student Privacy Pledge e membro do Future of Privacy Forum.

O RGPD é a nova legislação de proteção de dados da UE que substituirá a atual Diretiva de Proteção de Dados da UE 96/46 (Diretiva) e a implementação de Atos de Proteção de Dados nos Estados Membros da UE (por exemplo, o Ato de Proteção de Dados do Reino Unido, 1998).

O RGPD foi promulgado em maio de 2016 com uma data de cumprimento de 25 de maio de 2018.

Nas seções abaixo, fornecemos uma breve visão geral (e longe de totalmente abrangente) dos requisitos do RGPD. Você pode encontrar links para orientações mais detalhadas na seção "Recursos úteis sobre o RGPD".

Por que uma nova lei?

Os legisladores e reguladores da UE estavam convencidos de que a Diretiva precisava de atualização para abordar a falta de harmonização e os desenvolvimentos societais e tecnológicos ocorridos nos 20 anos desde a Diretiva. No topo da lista de prioridades estavam poderes de aplicação da lei mais fortes, alcance territorial mais amplo e direitos aprimorados para os indivíduos.

Muitas das novas disposições (por exemplo, efeitos extraterritoriais) destinam-se principalmente a redes sociais e empresas de Internet fora da UE. Os legisladores e reguladores da UE consideraram que a Diretiva atual não protegia suficientemente os direitos de privacidade de dados dos indivíduos da UE que utilizam tais redes sociais e serviços na internet.

A Blackboard opera de maneira diferente destas redes sociais e de outras empresas da Internet, cujo modelo é baseado na "monetização" dos dados dos usuários. Nós coletamos e usamos informações pessoais[2] de nossos clientes na direção dos mesmos e para fornecer nossos produtos e serviços para eles e seus usuários. Não coletamos nem usamos informações pessoais para vender essas informações ou para vender publicidade. Entendemos que a informação pessoal é confiada a nós e vem com obrigações. Portanto, temos um interesse compartilhado e uma responsabilidade compartilhada com nossos clientes em salvaguardar essas informações.

O que há de novo?

Embora baseado nos princípios e conceitos já existentes de privacidade de dados na UE, o RGPD traz alterações significativas ao regime de privacidade de dados na UE, incluindo:

- Maior poder de multas, em até 4% do faturamento global ou 20 milhões de euros (o que for maior)
- Extensão do âmbito territorial a organizações fora da UE que fornecem produtos e serviços a residentes da UE ou monitorizam residentes na UE
- Notificação de violação obrigatória às autoridades de supervisão no prazo de 72 horas para os controladores de dados[3]
- Requisitos mais rigorosos em relação ao consentimento
- Direitos aprimorados por parte dos indivíduos (incluindo o direito de apagar os dados e portabilidade de dados)

Mas algumas das mudanças mais importantes são os novos princípios de responsabilização e privacidade desde a concepção. Esses princípios exigem uma governança e processos de privacidade de dados eficazes, além de documentação mais detalhada e robusta sobre como uma organização atende aos requisitos do RGPD.

O que continua igual?

Muitos dos conceitos e definições do RGPD permanecem os mesmos ou são semelhantes em comparação com a Diretiva:

- A definição de "dados pessoais" (ou informações pessoais) permanece basicamente a mesma, mas agora inclui explicitamente endereços de IP, cookies e identificadores de dispositivos
- Os conceitos de "controlador de dados" e "processador de dados" permanecem os mesmos (mas o RGPD impõe responsabilidades mais diretas aos processadores de dados)[4]
- Os princípios de processamento estabelecidos na Diretiva (por exemplo, processamento legal e justo, limitação das finalidades, manutenção dos dados pessoais durante somente o tempo necessário) são mantidos
- Os requisitos de transferência de dados permanecem basicamente os mesmos: transferências de dados fora da UE/EEA são permitidas desde que seja usado um mecanismo de transferência de dados aprovado (por exemplo, Escudo de Proteção da Privacidade UE-EUA ou "cláusulas modelo")[5]

O nível mais alto de multas sob o RGPD significa que a não conformidade com os princípios e requisitos existentes, como apenas manter os dados pessoais pelo tempo necessário ou ter as medidas de segurança adequadas, provavelmente acarretará em um risco maior.

Qual o impacto do Brexit?

O RGPD será diretamente aplicável no Reino Unido a partir de 25 de maio de 2018 até o 'Brexit', no final de março de 2019. No entanto, mesmo após o Brexit, o RGPD estabelecerá o padrão no Reino Unido:

- O governo do Reino Unido publicou o UK Data Protection Bill 2017 (atualmente em processo legislativo) que implementa o RGPD antes e depois do Brexit[6]
- Após o Brexit, o RGPD aplicar-se-á diretamente às organizações britânicas que oferecem bens e serviços a residentes da UE ou os monitoram (por exemplo, universidades do Reino Unido que recrutam ativamente estudantes da UE)

Impacto nas transferências de dados de e para o Reino Unido:

- A UE esclareceu que, após o Brexit, o Reino Unido será considerado um "país terceiro", o que significa que não é mais considerado um país "adequado" (lista branca) para transferências de dados.
- A menos que e até que o Reino Unido seja declarado adequado pela Comissão da UE (por exemplo, como parte de um acordo transitório), acordos de transferência de dados ou outro mecanismo de transferência de dados precisam ser implementados para transferências de informações pessoais da UE para o Reino Unido.
- Por outro lado, o Reino Unido precisa determinar quais países considera autorizados (o que provavelmente incluiria os países da UE e os países listados na lista branca da UE). Para os países que não são considerados adequados, os mecanismos de transferência de dados reconhecidos pelo Reino Unido (provavelmente semelhantes aos mecanismos da UE) terão de ser utilizados para transferências de informações pessoais para fora do Reino Unido.

Desmistificando o RGPD

Um dos objetivos do RGPD era fornecer mais clareza por meio de uma prescrição mais detalhada. No entanto, ainda há muitos aspectos do RGPD que estão abertos a interpretação. Além disso, a complexidade do RGPD levou a uma falta de compreensão, bem como a afirmações exageradas. Isto deu origem a muitos mitos, alguns dos quais desmistificamos abaixo:[7]

Mito 1: É necessário consentimento para todo processamento de informações pessoais

Fato: O consentimento é apenas uma das várias bases legais que permitem o processamento de informações pessoais (por exemplo, o processamento necessário para a execução de um contrato ou em "interesse legítimo" de uma organização). O padrão de consentimento tornou-se muito alto. Por exemplo, a menos que os indivíduos possuam livre escolha genuína e possam retirar seu consentimento a qualquer momento, sem qualquer desvantagem, isso não será considerado um consentimento válido. Em muitos cenários de processamento de dados, outras bases legais serão mais adequadas.[8]

Mito 2: As 72 horas de período de notificação de violação aplicam-se a toda a cadeia de fornecimento (ou seja, a partir do momento em que um (sub)processador está ciente da violação)

Fato: O RGPD exige que os processadores de dados notifiquem seu controlador de dados "sem atrasos indevidos" no caso de uma violação de dados pessoais. Somente após o processador de dados ter notificado o controlador, o período de notificação de 72 horas para o controlador de dados é iniciado. O Grupo de Trabalho do Artigo 29 (WP29), o grupo de autoridades de proteção de dados da UE, esclareceu em suas orientações finais[9] que "sem atraso indevido" significa notificação "rápida" (não notificação "imediata" como sugerido em um rascunho anterior).

Mito 3: Transferências de dados fora da UE/EEE não são permitidas ou são permitidas somente com o consentimento do cliente para cada transferência de dados

Fato: O RGPD retém amplamente os requisitos de transferência de dados existentes. Como tal, as transferências de dados são permitidas se um mecanismo de transferência de dados aprovado pela UE, como o Escudo de Proteção da Privacidade UE-EUA ou as cláusulas modelo aprovadas pela UE (acordos de transferência de dados) estiverem em vigor. A Blackboard possui esses dois mecanismos para transferir as informações pessoais[10] dos clientes. Como a Blackboard atua como um processador de dados, é necessária uma instrução geral para transferências de dados dos clientes (que está contida em nosso contrato padrão de processamento de dados), mas as autorizações do cliente para cada transferência de dados não são necessárias.

Mito 4: O direito de apagar exige que as organizações excluam todos os dados sobre um indivíduo

Fato: O novo direito de apagar não é um "direito absoluto de ser esquecido". Em vez disso, é um direito de ter os dados excluídos se os dados não forem mais necessários e em outras circunstâncias em que a organização não atenda aos requisitos do RGPD. Se uma organização ainda precisa legitimamente reter os dados (por exemplo, devido a requisitos de retenção de registros), essas informações pessoais não precisam ser excluídas.

Mito 5: O RGPD aplica-se a todas as universidades que têm estudantes da UE

Fato: Apenas ter alunos da UE inscritos não é suficiente para a aplicabilidade do RGPD. O RGPD geralmente se aplica a instituições estabelecidas na UE. Aplica-se também a universidades fora da UE, mas apenas se oferecerem bens e serviços a indivíduos na UE ou se monitorarem o comportamento de indivíduos na UE. Para que se considere que "oferece-se serviços" é preciso algum grau de direcionamento. O simples fato de estudantes da UE estarem matriculados não é suficiente. O RGPD pode, no entanto, aplicar-se quando as universidades se direcionam ativamente a residentes na UE (por exemplo, para cursos on-line) ou recrutam ativamente estudantes em países da UE. Esses critérios estão abertos a interpretação. Recomendamos aos clientes que obtenham seu próprio aconselhamento jurídico.

IMPLEMENTANDO O RGPD

Porque é importante entender privacidade de dados e o RGPD corretamente

O risco de 4% de multas globais no volume de negócios é certamente uma razão pela qual muitas organizações começaram a levar mais a sério a privacidade de dados. Mas achamos que o argumento positivo para boas práticas de privacidade de dados é pelo menos tão convincente quanto este, porque a privacidade de dados é um direito humano, e porque práticas robustas de privacidade de dados cria confiança.

Na sociedade atual, a informação pessoal está em toda parte. A informação pessoal é frequentemente chamada de "o novo petróleo da economia". Todos nós utilizamos serviços online e entregamos nossas informações pessoais. Mas estudos após estudos mostram que as organizações não são confiáveis quando se trata de informações pessoais. Há uma sensação de que os indivíduos perderam o controle sobre seus dados. Legisladores e reguladores estão reagindo a tal. O RGPD é provavelmente o exemplo mais proeminente. As organizações precisam (re)conquistar a confiança dos indivíduos. Boas práticas de privacidade de dados são fundamentais para construir essa confiança. Elas também constituem uma vantagem competitiva. Por último, elas também ajudam as organizações com inovação. Se os alunos (e funcionários) confiam em sua instituição, eles estarão mais propensos a compartilhar suas informações e a usar novas ferramentas.

Uma compreensão incorreta de privacidade de dados pode ser catastrófica. Violações de dados aparecem regularmente entre as notícias. O que vem a seguir são danos à reputação, a perda de confiança dos indivíduos e o risco de acusações por parte daqueles cujos dados foram mal administrados. As autoridades de proteção de dados podem não aplicar multas de 4% sobre volume de negócios desde o início, mas têm muitas outras ferramentas de aplicação da lei à sua disposição e podem forçar as instituições a alterar suas práticas de dados e implementar programas de privacidade de dados com auditorias externas regulares.

O papel de nossa e de sua organização sob o RGPD

O RGPD mantém o conceito de "controlador de dados" e "processador de dados". Este conceito é crucial, pois determina as obrigações e responsabilidades das organizações e seus prestadores de serviços.

Uma organização é considerada um controlador de dados se determinar os "meios e propósitos" do processamento de informações pessoais, ou seja, porque e como as informações pessoais são usadas. O processador de dados, por outro lado, é a organização que atua em nome do controlador de dados e sob sua instrução.

Para a maioria dos produtos e serviços da Blackboard (por exemplo, Learn, Collaborate, Open LMS), a Blackboard é considerada um processador de dados e, nossos clientes, o controlador de dados.

O RGPD impõe requisitos mais diretos aos processadores de dados, como a Blackboard. No entanto, a maioria dos requisitos do RGPD ainda se aplica aos controladores de dados (por exemplo, a responsabilidade de informar os indivíduos sobre como os dados estão sendo usados, atender às solicitações individuais de acesso aos dados, notificação de violação obrigatória às autoridades de proteção de dados e indivíduos).

O que você pode fazer para se preparar para o RGPD?

Todas as organizações incluídas no escopo do RGPD deverão estar preparadas até 25 de maio de 2018. Aqui estão alguns itens importantes que os clientes podem fazer para se prepararem. Esta lista de etapas tem por base nossa própria experiência e não pretende, de forma alguma, ser completamente abrangente. Por favor, certifique-se de envolver especialistas em privacidade de dados para ajudá-lo com sua implementação. Muitas autoridades de proteção de dados também criaram suas orientações sobre como implementar o RGPD.[11]

É possível que você já tenha implementado as etapas 1-6 e esteja no meio da implementação de seus planos de ação. Mas nunca é tarde para começar. Mesmo se você acabou de começar, pode implementar as mudanças mais críticas. Isso também significa que você será capaz de demonstrar à sua autoridade de proteção de dados que está trabalhando em um plano. Ignorar o RGPD não é uma opção.

1. **Verifique se o RGPD se aplica à sua organização**

   Se a sua organização está estabelecida na UE, então o RGPD se aplica. O RGPD também pode, porém, se aplicar a organizações fora da UE.[12]

2. **Estabeleça um projeto de RGPD**

   Projetar e implementar um projeto dedicado ao RGPD. Em um cenário ideal, você terá suporte ao gerenciamento de projetos e contatos designados que podem apoiá-lo em todos os departamentos. Este projeto abrangerá todos os departamentos de sua instituição e você precisará de ajuda.

3. **Indique um líder em RGPD com experiência para gerenciar o projeto**

   O líder não deve ser apenas um líder de privacidade de dados experiente, mas também ter tempo e recursos suficientes, bem como acesso a suporte externo (por exemplo, um escritório de advocacia). Se a sua organização é uma autoridade pública estabelecida na UE, você também precisará nomear um Diretor de Proteção de Dados.

4. **Garanta a adesão e a supervisão da alta administração**

   A implementação de um projeto de RGPD sem o apoio, direção e supervisão da alta administração é difícil.

5. **Analise seu uso de informações pessoais e conduza análises de lacunas**

   Entender onde e como as informações pessoais são usadas e onde os aprimoramentos para o RGPD são necessários é a primeira fase principal do projeto de RGPD.

6. **Desenvolva planos de ação para diminuir as lacunas**

   Esta é provavelmente a parte mais difícil do RGPD, pois requer a tradução dos requisitos de alto nível do RGPD em ações específicas e praticáveis para todos os vários processos e sistemas.

7. **Implemente planos de ação**

   É bom confiar, mas, neste caso, é melhor controlar. Esta fase requer o acompanhamento dos planos de ação de outros para garantir que eles estejam cumprindo seus prazos.

8. **Analise junto a seus fornecedores**

   Sob o RGPD você é responsável por seus fornecedores. Ter as cláusulas contratuais certas em vigor é importante, mas não suficiente. Você precisa estar confiante de que seus fornecedores estão atendendo aos requisitos do RGPD e podem oferecer suporte ao seu cumprimento. Pergunte-os como estão implementando o RGPD.

9. **Mantenha-se a par dos desenvolvimentos legais/regulamentares (diretrizes do Grupo de Trabalho do Artigo 29, leis de implementação dos Estados Membros)**

   Conhecer o RGPD é o suficiente, correto? Errado! Embora o RGPD seja aplicado diretamente, todos os Estados-Membros da UE estão implementando leis nacionais suplementares de proteção de dados. Estes são necessários para regular áreas onde os Estados Membros têm autoridade legislativa (por exemplo, privacidade de dados de funcionários) ou onde o RGPD lhes permite legislar ainda mais (por exemplo, critérios para DPOs e DPIAs). Além disso, o WP29 está publicando orientações importantes. Manter-se atualizado é desafiador, mas importante.[13]

PLANO E ABORDAGEM DA BLACKBOARD

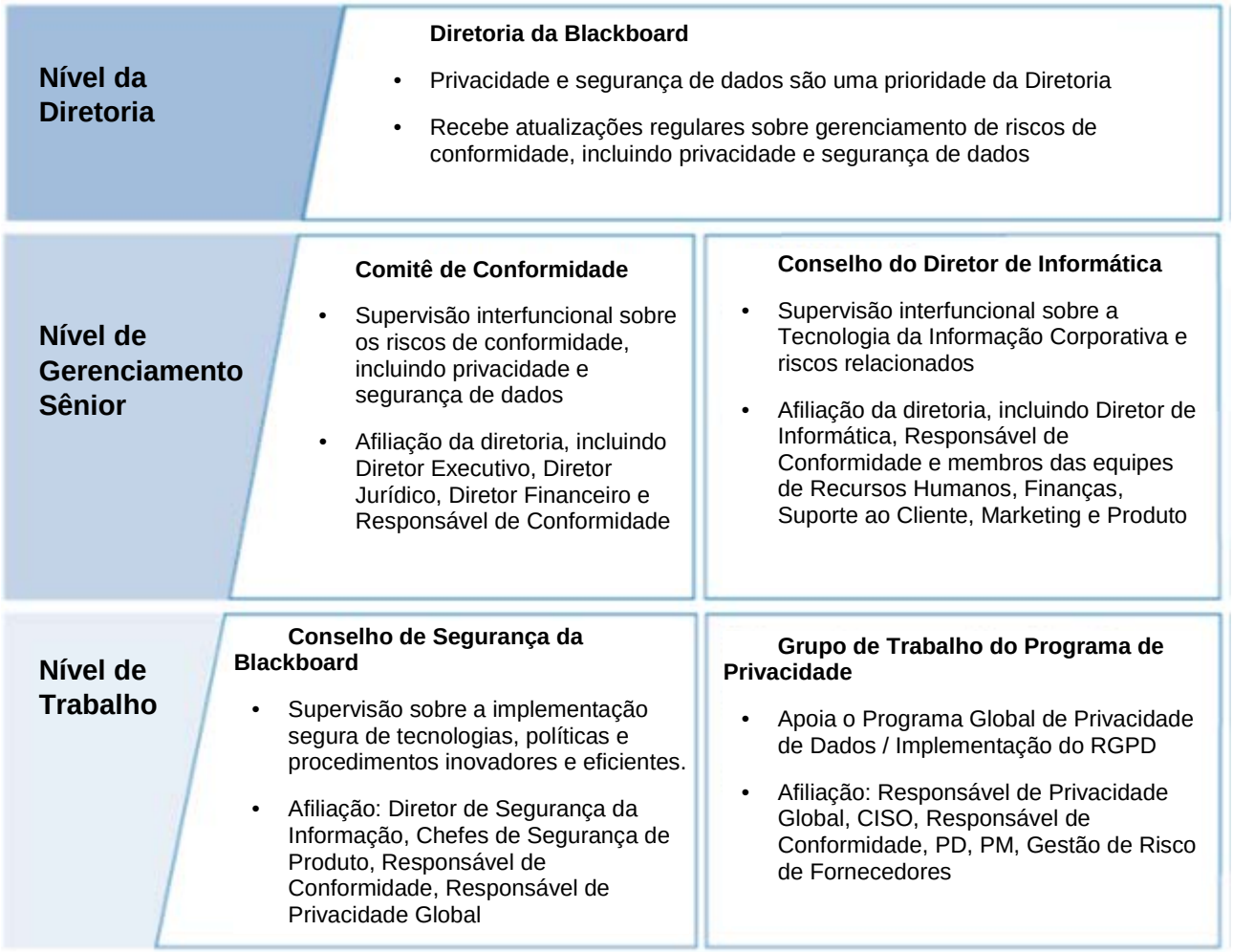
Privacidade e segurança de dados na Blackboard

A privacidade e a segurança de dados têm sido uma prioridade chave de longa data da Blackboard. Para nós, o RGPD é uma oportunidade para fortalecer ainda mais nossas práticas de privacidade de dados existentes.

Nossa abordagem à privacidade de dados sempre foi focada no cliente. Entendemos os desafios que nossos clientes enfrentam e queremos ajudá-lo em relação a estes.

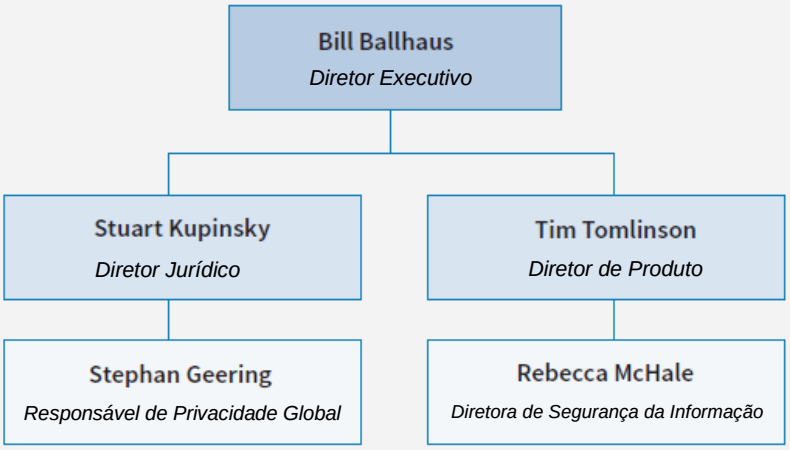
Boas práticas de privacidade de dados exigem um modelo de governança sólido. Na Blackboard, a privacidade e a segurança de dados são uma prioridade da diretoria e nosso modelo de governança (veja abaixo) garante que a gerência sênior supervisione e dê suporte aos nossos esforços de privacidade e segurança de dados.

A importância que a Blackboard dá à privacidade e à segurança de dados também é destacada pelo fato de nosso Responsável de Privacidade Global e nosso Diretor de Segurança da Informação[14] responderem à Equipe de Liderança do Diretor Executivo (veja o gráfico organizacional abaixo)



Privacidade e segurança

A importância que a Blackboard dá à privacidade e à segurança de dados também é destacada pelo fato de nosso Responsável de Privacidade Global e nosso Diretor de Segurança da Informação responderem à Equipe de Liderança do Diretor Executivo



Como a Blackboard aborda o RGPD

Estabelecemos um projeto abrangente para implementar os requisitos do RGPD usando a seguinte abordagem:

A implementação do RGPD baseia-se na experiência de privacidade de dados e nos mecanismos de conformidade existentes da Blackboard

- A implementação do RGPD é liderada pelo Responsável de Privacidade Global e apoiada por um gerente de projeto dedicado e "Líderes de RGPD" em cada área funcional
- O renomado escritório de advocacia Bristows LLP, entre vários outros, foi contratado para apoiar a implementação do RGPD
- A implementação do RGPD é supervisionada pelo Comitê de Conformidade da Blackboard, que inclui o Diretor Executivo da empresa, o Diretor Jurídico e outros oficiais superiores

O RGPD como uma oportunidade

Pensamos na implementação do RGPD não como um mero esforço para cumprir os novos requisitos de privacidade de dados da UE, mas também como uma oportunidade. Como tal, pretendemos usar a implementação do RGPD para realizar o seguinte:

- Fortalecer as práticas globais de privacidade de dados - usaremos o projeto do RGPD para aprimorar nosso programa global de privacidade de dados na UE e além
- Desenvolver processos de privacidade desde a concepção que reforcem a conformidade com privacidade de dados em nossos processos do dia-a-dia.
- Apoiar nossos clientes em seus esforços de conformidade com o RGPD
- Posicionar a Blackboard como o líder reconhecido em privacidade de dados em Tecnologia Educacional

Nosso plano de implementação

Estamos seguindo a metodologia de 3 fases estabelecida pela Bristow LLP para implementar nosso programa de Privacidade de Dados Global/RGPD. Essa metodologia está sendo usada por várias outras empresas, incluindo empresas líderes em tecnologia. As três fases principais são as seguintes:

- **FASE 1 - Coleta de informações**
- **FASE 2 - Desenvolvimento de soluções**
- **FASE 3 - Fluxos de trabalho de implementação**

Usamos essa metodologia de três fases para desenvolver nosso programa com os quatro estágios chave a seguir:

Iniciação de Projeto

O estágio de iniciação de projeto incluiu as seguintes atividades:

- Briefing e adesão da gerência sênior
- Contratação de um Responsável de Privacidade Global com a responsabilidade de liderar o projeto de RGPD
- Desenvolvimento de plano de projeto e governança de projeto
- Coleta inicial de informações e avaliação das atividades atuais de conformidade para áreas que exigem aprimoramentos no escopo do RGPD

FASE 1 - Coleta de Informações (Workshops)

Durante essa fase inicial, conduzimos conversas/workshops estruturados com os principais interessados das áreas funcionais e grupos de produtos da Blackboard para obter informações detalhadas sobre as práticas de processamento de dados nessas áreas.

O resultado dos workshops foi usado para realizar a análise de lacunas e desenvolver as soluções e os planos de implementação na fase 2.

FASE 2 - Desenvolvimento de soluções

Com base nas informações dos workshops, desenvolvemos as seguintes soluções e documentação:

- Documentação aprimorada de privacidade de dados interna (políticas e padrões operacionais detalhados) que refletem os requisitos do RGPD e explicam como os requisitos do RGPD terão de ser cumpridos para as várias atividades de processamento de dados (por exemplo, requisitos para processamento de dados do cliente, processo de privacidade desde a concepção)
- Requisitos de produto
- Planos de implementação para as áreas funcionais e para esforços centralizados necessários

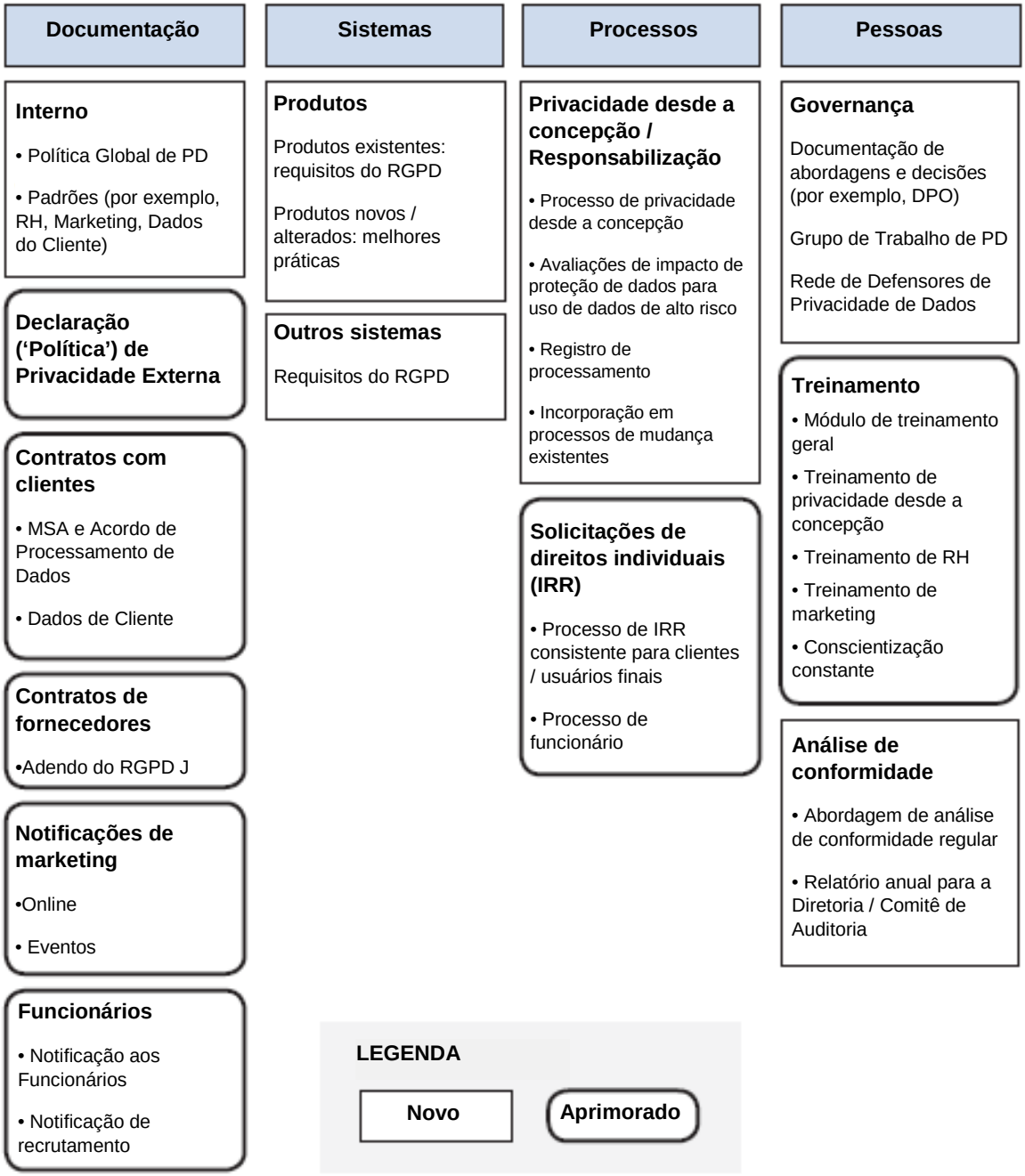
FASE 3 - Fluxos de trabalho de implementação

Durante a fase final, estamos implementando a documentação de privacidade de dados desenvolvida e executando os planos de implementação. Seis principais fluxos de trabalho serão usados para realizar a implementação:

1. Execução dos planos de implementação para as áreas funcionais e grupos de produtos
2. Revisão e atualização de políticas, avisos e consentimentos voltados ao público
3. Melhoria da governança (papéis e responsabilidades, treinamento, privacidade desde a concepção etc.)
4. Revisão e atualização de contratos de fornecedores (quando necessário) [15]
5. Alterações nos sistemas de TI (quando necessário)
6. Estabelecimento de registro de processamento de dados

Visão geral das mudanças

O gráfico abaixo mostra como visualizamos o estado final de nosso programa de privacidade de dados / RGPD após as atividades de implementação. Após a implementação do RGPD, continuaremos inovando e nos adaptando para amadurecer ainda mais nossas práticas de privacidade de dados.



COMO O NOSSO PROGRAMA DE RGPD O AJUDARÁ?

O programa de implementação de Privacidade Global de Dados / RGPD da Blackboard está focado em apoiar sua organização com sua implementação do RGPD. As seções a seguir fornecerão mais informações mas, em resumo, os sete pontos chave são:

1. **Produtos prontos para o RGPD:** Estamos implementando requisitos de produtos para apoiar clientes com requisitos de transparência, solicitações de direitos individuais etc.
2. **Privacidade desde a concepção:** Estamos implementando um processo de privacidade desde a concepção e de Avaliação de Impacto de Proteção de Dados (DPIA) para facilitar a documentação de conformidade.
3. **Transferências de dados:** Continuaremos a nossa abordagem multi-camadas: Regionalização, Escudo de Proteção de Privacidade UE-EUA e cláusulas modelo aprovadas pela UE
4. **Contrato com clientes:** Temos um adendo de processamento de dados pronto para o RGPD para nosso contrato-mestre padrão
5. **Nossos fornecedores:** Temos contratos robustos e uma estrutura de Gerenciamento de Risco de Fornecedores em vigor
6. **Segurança:** Estabelecemos políticas, procedimentos e governança que são continuamente aprimorados para salvaguardar a segurança dos dados de cliente.
7. **Notificação de violação:** Temos um processo de Resposta a Incidentes de Segurança documentado e testado

1. Produtos prontos para o RGPD

Apoiar nossos clientes tornando nossos produtos prontos para RGPD é um dos aspectos chave de nossos fluxos de trabalho de implementação. Para esse fim, criamos requisitos mínimos de privacidade de dados/RGPD para nossos produtos. Alinhados com nossa abordagem em fortalecer nossas práticas de privacidade de dados globalmente, a maioria desses requisitos se aplica a todos os nossos produtos, não apenas aos produtos que disponibilizamos na UE. Isto também auxilia os nossos clientes fora da UE que podem cair no escopo do RGPD.

Desenvolvemos nossos requisitos de produtos de privacidade de dados/RGPD por meio de um processo robusto e intensivo. Elaboramos uma versão inicial com um consultor externo. Durante várias sessões de trabalho e revisões com as principais partes interessadas de nossas equipes de desenvolvimento de produtos e gerenciamento de produtos, refinamos a versão em requisitos gerais de produtos específicos e acionáveis, com orientação detalhada. Os requisitos de produto de privacidade de dados/RGPD foram posteriormente traduzidos em ações específicas de produto nos planos de implementação de produto para cada grupo de produtos.

Nossos requisitos de produto[16] podem ser categorizados da seguinte forma:

Transparência

- Capacidade de os clientes vincularem-se a suas políticas/notificações de privacidade
- Fornecimento de informações sobre como as informações pessoais geralmente estão sendo usadas em um produto

Minimização / exclusão de dados

- Análise de produtos quanto a campos desnecessários / opcionais
- Análise de produtos quanto a oportunidades de uso de dados anônimos ou pseudônimos em vez de informações pessoais
- Capacidade de excluir informações pessoais quando solicitadas por clientes (quando clientes / usuários não podem excluir os dados)

Direitos individuais gerais

- Capacidade de fornecer acesso e corrigir informações pessoais quando solicitado por indivíduos
- Capacidade de excluir informações pessoais quando solicitado por indivíduos

Direitos individuais da UE

- Capacidade de lidar com solicitações de portabilidade de dados (direito de os indivíduos receberem dados em formato legível por máquina em certas circunstâncias)
- Capacidade de parar de usar informações pessoais (direito de oposição / direito à restrição em determinadas circunstâncias)

A Blackboard já possui programas definidos para a segurança de nosso produto que levam em conta o RGPD. Portanto, não definimos requisitos de segurança específicos para o RGPD adicionais.[17]

2. Privacidade desde a concepção

À medida que se torna cada vez mais desafiador para os indivíduos manterem o controle sobre suas informações (veja postagem sobre esse assunto em nosso **blog diário de privacidade**), a privacidade desde a concepção e a responsabilização se tornam cada vez mais importantes para manter a confiança dos indivíduos, clientes e órgãos reguladores para documentar como uma organização está em conformidade com o RGPD. Estamos, portanto, colocando nossa abordagem de privacidade desde a concepção no centro do nosso programa de Privacidade de Dados Global / RGPD.

Para a Blackboard, isso é uma evolução e não uma revolução. Desde sempre conduzimos análises legais de novos produtos e práticas. Com a nossa abordagem de privacidade desde a concepção, estamos formalizando e documentando melhor essas análises.

Abordagem

- Criamos um processo e uma lista de verificação documentados de privacidade desde a concepção.
- Áreas funcionais e grupos de produtos estão incluindo a lista de verificação de privacidade desde a concepção em seus processos de mudança.
- Toda mudança material na forma como as informações pessoais são usadas requer o cumprimento da lista de verificação de privacidade desde a concepção. Embora não seja especificamente requerida pelo RGPD, essa é a melhor prática.
- A lista de verificação irá desencadear uma Avaliação de Impacto de Proteção de Dados (DPIA) para uso de alto risco de informações pessoais (requisito do RGPD)

O fluxograma abaixo exibe a abordagem:

3. Transferências de dados

O RGPD não traz alterações significativas no modo como as informações pessoais podem ser transferidas para fora da UE/EEE. As atuais restrições e mecanismos de transferência de dados permanecem. Isto significa que as transferências de dados são permitidas se um mecanismo de transferência de dados aprovado pela UE, como o Escudo de Proteção da Privacidade UE-EUA ou as cláusulas modelo aprovadas pela UE (acordos de transferência de dados) estiverem em vigor. Esses mecanismos garantem que as informações pessoais sejam adequadamente protegidas, mesmo quando saem da UE/EEE.

Continuaremos com nossa abordagem de várias camadas e de redundância para a conformidade de transferência de dados. Isso significa que abordamos os requisitos de transferência de dados por meio de várias vias de modo a garantir que as proteções adequadas estejam em vigor para suas informações:

- **Hospedagem Regional:** Temos uma estratégia de hospedagem regional com quase todos os produtos hospedados na UE e outros produtos sob planejamento de serem movidos para soluções de hospedagem regional. Embora a hospedagem regional não seja exigida pelo RGPD e não acreditemos que a localização de dados leve a uma melhor privacidade ou segurança de dados[18], entendemos que muitos clientes da UE preferem que seus dados sejam armazenados na UE.
- **Escudo de Privacidade:** A Blackboard é certificada pelo Escudo de Proteção da Privacidade UE-EUA, o que nos permite transferir legalmente dados pessoais para os EUA.
- **Cláusulas modelo:** Também utilizamos acordos de "cláusula modelo" aprovados pela UE, que nos permitem transferir, de maneira conforme, dados pessoais para fora do EEA dentro do grupo de empresas da Blackboard ("Contrato de transferência de dados de cliente").
- **Fornecedores:** Contratos robustos estão em vigor com fornecedores e parceiros (por exemplo, IBM, Amazon Web Services) para garantir que os requisitos de transferência de dados (e outras obrigações de proteção de dados) sejam repassados aos nossos fornecedores e parceiros.

Nós atualmente[19] temos vários centros de dados regionais para apoiar o tratamento de dados na UE para os nossos clientes da UE:

- Hospedagem gerenciada (centros de dados da Blackboard): Centros de dados em Amsterdã (Holanda) e Frankfurt (Alemanha).
- Hospedagem na nuvem (data center da AWS): AWS região de Frankfurt, Alemanha (eu-central-1).

Os centros de dados da AWS atendem a uma série de certificações e requisitos de ISO 27001 e ISO 27018, à SOC2 e à conformidade com o RGPD, além da conformidade com os requisitos locais, como o C5 alemão e o IT-Grundschutz.[20]

É importante compreender que enquanto as informações pessoais dos clientes são armazenadas nesses centros de dados para a maioria dos produtos (incluindo Learn 9.1, Learn SaaS, Open LMS e Collaborate) para clientes da UE, o acesso a esses dados fora da UE / EEA pode ser necessário para fornecer os produtos e serviços, por exemplo, para suporte 24 horas por dia, 7 dias por semana. Tais transferências de dados são permitidas graças às mencionadas cláusulas de certificação e modelo do Escudo de Proteção da Privacidade UE-EUA.

4. Contratos com clientes

A Diretiva atual exige que um controlador de dados tenha um contrato em vigor com o fornecedor (processador de dados), mas não prescreve o conteúdo do contrato em detalhes. O RGPD é mais prescritivo e inclui uma lista de conteúdo obrigatório.[21]

Nosso adendo atual de processamento de dados padrão inclui todos os pontos requeridos abaixo. Ele é incluído automaticamente para clientes em nosso contrato mestre padrão que se encontram no escopo do RGPD.

- ✓ Use dados pessoais somente conforme instruído
- ✓ A equipe deve assinar acordos de confidencialidade
- ✓ Medidas de segurança adequadas devem estar em vigor
- ✓ Somente engaje fornecedores (subprocessadores) ...
    - Conforme autorizado pelo controlador de dados (pode ser uma autorização geral)
    - Que sejam contratualmente obrigados a seguir as mesmas obrigações de proteção de dados
- ✓ Forneça assistência ao controlador na resposta a solicitações de direitos individuais
- ✓ Forneça assistência ao controlador com medidas de segurança, notificação de violação e avaliações de impacto de proteção de dados
- ✓ Retorne ou excluir dados no final do contrato
- ✓ Forneça informações necessárias para o controlador de dados para demonstrar conformidade
- ✓ Informe imediatamente o controlador de dados se alguma instrução do controlador de dados violar o RGPD

5. Gerenciamento dos nossos fornecedores

A Blackboard usa fornecedores (por exemplo, IBM, Amazon Web Services) para nos ajudar a fornecer nossos produtos e serviços para nossos clientes. Caso precise de acesso às informações pessoais de nossos clientes, a Blackboard é responsável pelas práticas de privacidade de dados dos fornecedores.

Como parte de nosso programa RGPD, estamos conectando intimamente a abordagem da concepção com os processos existentes de Gerenciamento de Risco e Aquisição de Fornecedores. Isso resulta nos controles chave dispostos a seguir:

- Contratos robustos com um Adendo de privacidade e RGPD em vigor com terceiros, impondo disposições materialmente equivalentes que temos em vigor com nossos clientes
- Acordos sobre "Cláusula modelo" e/ou Adendo ao RGPD e Proteção à Privacidade para possibilitar transferências de dados legais para nossos fornecedores
- Política e estrutura de Gerenciamento de Risco do Fornecedor Documentado
- Novos fornecedores com acesso a informações pessoais precisam preencher um Questionário de Avaliação de Segurança do Fornecedor com perguntas referentes ao cumprimento da privacidade
- Os fornecedores com acesso aos sistemas gerenciados pela Blackboard são obrigados a seguir as políticas de controle de acesso e identidade e autorização da Blackboard, para incluir revisões de conta, conforme apropriado.
- Os fornecedores precisam acessar os recursos da Blackboard por meio de mecanismos aprovados (por exemplo, VPN)
- Os fornecedores restringiram os controles de acesso ao tráfego, usuários e ativos

6. Segurança

O RGPD não altera materialmente as medidas técnicas e operacionais ("TOMs") para a segurança das informações pessoais. Essas medidas devem ser "adequadas" ao risco envolvido, conforme previsto na Diretiva em vigor. Portanto, continuamos a confiar em nossos programas de segurança da informação estabelecidos.

Administração do risco de segurança da informação

Estabelecemos políticas, procedimentos, governança e exigências técnicas para gerenciar o risco de segurança de TI em toda a empresa.

Desde o primeiro dia, a equipe da Blackboard deve entender sua responsabilidade de proteger os dados pessoais do cliente:

- Reconheça a política para proteger informações confidenciais
- Treinamento anual em segurança de usuários e privacidade de dados
- Exercícios de phishing
- Boletins de conscientização

As seguintes exigências estão em vigor para a proteção de dados por nossa equipe:

- As classificações de dados são definidas com exigências para proteger cada tipo de dado. Os dados do nosso cliente, os dados das instituições e de seus alunos têm a maior sensibilidade.
- Os controles técnicos estão em vigor para proteger os dados, por exemplo:
    - uso de criptografia
    - atualizações de segurança imediatas
    - controles de autenticação aprimorados
    - proteção contra tráfego na web e email mal-intencionado
    - tecnologias de proteção de endpoint
    - acesso restrito com base na necessidade de conhecer

Não é apenas o RGPD...

Como uma empresa global, que serve a comunidade educacional, monitoramos de perto as leis e regulamentos de privacidade e segurança de dados específicos do setor educacional e geográfico.

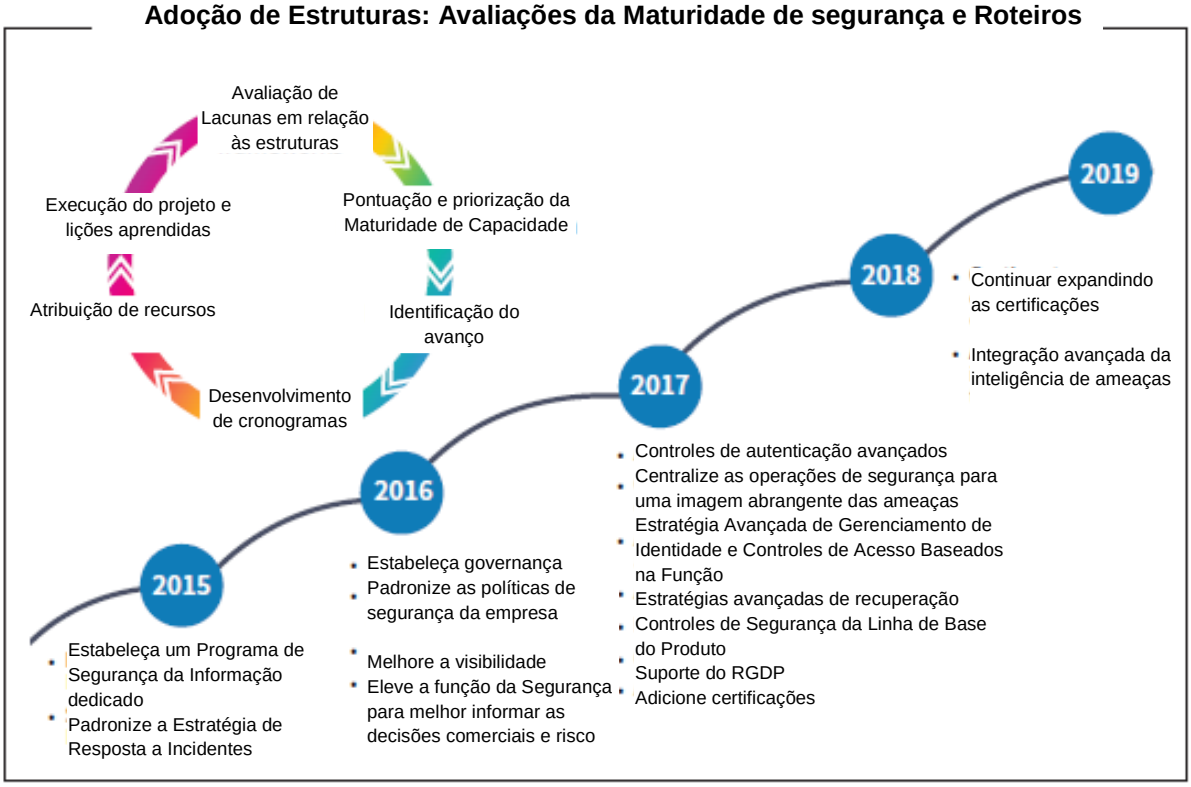
A lista abaixo é apenas alguns exemplos de regulamentos, normas e estruturas de segurança e privacidade de dados que a Blackboard leva em consideração, além do RGPD, ao desenvolver nossas políticas de segurança, processos e controles técnicos.

- Lei de Direito e Privacidade da Educação Familiar dos EUA (FERPA), Emenda de Direitos à Proteção de Alunos (PPRA)
- Lei de Proteção à Privacidade On-line das Crianças dos EUA (COPPA)
- Leis Estaduais dos EUA (colcha de retalhos existente e emergente de 50 estados)
- Normas do Governo dos EUA - FedRAMP
- Normas de Segurança de Dados de PCI, se aplicável
- ISO/IEC, OWASP, NIST
- Normas internacionais (MTCS, IRAP)

Avaliações e roteiros da maturidade de segurança

Trabalhamos duro para melhorar continuamente nossas medidas de segurança técnica e operacional. O diagrama da próxima página apresenta nossas avaliações de maturidade contínuas e nossos roteiros.

Adoção de Estruturas: Avaliações da Maturidade de segurança e Roteiros



7. Notificação de Violação

Uma das principais mudanças do RGPD é a nova notificação obrigatória de violações de dados pessoais à autoridade de proteção de dados competente e (em alguns casos) aos indivíduos afetados.[22]

Para a maioria dos nossos produtos e serviços, a Blackboard é um processador de dados[23] de acordo com o RGPD. A obrigação de notificar as autoridades de proteção de dados e os indivíduos em caso de violação que envolva a Blackboard seria, portanto, dos nossos clientes. No entanto, o RGPD exige que os processadores de dados, como a Blackboard, notifiquem seus clientes (controladores de dados) sem demora injustificada (ou seja, "imediatamente")[24] nesse caso.

Temos as seguintes medidas em vigor que apoiam nossos clientes no cumprimento de suas obrigações no caso de uma violação de dados pessoais na Blackboard relacionada a um cliente:

- Processo de Resposta a Incidentes de Segurança (SIR) da Blackboard
  - Documentado e testado regularmente
  - Facilita a rápida identificação, investigação e remediação em caso de incidente
  - Permite notificações rápidas aos clientes
  - Depende da equipe de resposta a incidentes de segurança estabelecida (que inclui o Diretor de Segurança da Informação e o Responsável de Privacidade Global)
- Nossa obrigação de notificar os clientes imediatamente é expressamente declarada em nosso contrato mestre padrão vigente e adendo de proteção de dados.[25]

CONCLUSÃO

O RGPD exige alterações significativas com impacto para além da data de cumprimento de 25 de maio de 2018. Esperamos que este informe possa contribuir para a implementação bem-sucedida do RGPD e que tenha demonstrado como a Blackboard leva a sério o RGPD e o cumprimento da privacidade de dados.

As próximas seções apresentam informações úteis adicionais e listam nosso e-mail de contato caso tenha qualquer dúvida ou comentário referente a este informe.

RECURSOS ÚTEIS DO RGPD

Os links dos recursos abaixo são apenas uma pequena seleção de material útil disponível off-line. Não pretende ser uma lista abrangente.

Para uma análise detalhada sobre como o RGPD se aplica a você, você também deve buscar informações dos especialistas. É importante contar com especialistas experientes em proteção de dados (por exemplo, em seu escritório de advocacia

Recursos Oficiais da UE

- Texto do RGPD
- Diretrizes do Grupo de Trabalho do Artigo 29
- Website da Comissão do RGPD da UE

Materiais da Autoridade de Proteção de Dados da UE

- O Escritório do Comissariado da Informação do Reino Unido (ICO) tem um excelente site de RGPD com material útil em linguagem simples que é constantemente atualizado
- O Comissariado de Proteção de Dados da Irlanda (DPC) tem uma página de RGPD dedicada para organizações
- O CNIL francês fornece algum material em inglês, incluindo um software gratuito de Avaliação de Impacto da Privacidade (e muito mais material em francês)
- A AEPD espanhola produziu um guia para instituições de ensino (PDF, em espanhol)

Guias de escritórios de advocacia

- Bird & Bird's guide to the GDPR
- Bird & Bird's Member State laws tracker (variações nacionais de rastreamento de RGPD)
- Linklaters' GDPR survival guide (PDF)
- White & Case GDPR handbook

Outras organizações

- A JISC UK tem recursos úteis, eventos e atualizações de blog sobre RGPD
- A UCISA publicou um documento de boas práticas de RGPD com etapas práticas e estudos de caso
- A Associação Internacional de Profissionais de Privacidade (IAPP) tem um bom boletim informativo semanal (gratuito) sobre a evolução da privacidade de dados na Europa
- O IAPP também oferece uma visão geral útil dos prestadores de ferramentas de privacidade de dados (PDF)
- A Amazon Web Services tem um Centro de RGPD dedicado

BIOGRAFIAS

Stephan Geering

Responsável de Privacidade Global

- Responsabilidade global pela conformidade com as leis de privacidade e segurança de dados
- Lidera o Programa Global de Privacidade de Dados / Implementação do RGPD
- Responde ao Diretor Jurídico; membro da equipe Jurídica da Blackboard
- Localizado em Londres

Sobre Stephan:

- Advogado / Comissário Adjunto de Proteção de Dados em uma Autoridade de Proteção de Dados dos Cantões da Suíça (2002-2008)
- Mestre em Direito, LLM pela University College London (2008-2009)
- Diretor Associado, Grupo de Privacidade em Barclays (2010-2012)
- Chefe Regional EMEA de Operações de Privacidade de Dados no Citigroup (2012-2014)
- Diretor de Privacidade EMEA e APAC no Citigroup (2014-2017)
- Certificado CIPP/E

Rebecca McHale

Diretora de Segurança da Informação

- Lidera estratégia de segurança para produtos e infraestrutura
- Supervisiona a governança da segurança cibernética da Blackboard
- Subordinado ao Diretor de Produtos
- Localizada em Washington, D.C.

Sobre Rebecca:

- Entrou na Blackboard em 2016; recentemente, combinou as equipes de segurança e elevou a função da organização de segurança dentro da empresa
- Mestra (MS) em Matemática Discreta e Aplicações de Computação pela Royal Holloway,
  Universidade de Londres
- Anteriormente, Diretor Sênior de Programas Cibernéticos em Novetta e CSRA, atendendo clientes governamentais e comerciais dos EUA, por exemplo: Department of State, Transportation Security Administration (TSA), e Federal Deposit Insurance Corporation (FDIC)

INFORMAÇÕES ADICIONAIS

Você pode encontrar mais informações sobre nossa página dedicada à privacidade e segurança de dados.
Também temos um Boletim Informativo sobre Privacidade de Dados. Se você gostaria de receber nossa newsletter ou tiver alguma dúvida ou feedback sobre este artigo, por favor, entre em contato conosco em privacy@blackboard.com.

Fontes

1 Consulte a seção "Recursos úteis sobre o RGPD" no final deste documento para obter orientações mais detalhadas sobre o RGPD.

2 Preferimos o termo "informação pessoal" a "dados pessoais", mas o empregamos com o mesmo significado e escopo que "dados pessoais".

3 O controlador de dados é a organização que determina os meios e propósitos do processamento de dados (como e porque as informações pessoais são usadas).

4 Veja a seção "O papel de nossa e de sua organização sob o RGPD".

5 Consulte a seção "Desmistificando o RGPD" abaixo para obter mais detalhes sobre transferências de dados.

6 Consulte a "Introdução à Lei de Proteção de Dados" da OIC, para uma visão geral da lei.

7 Veja também as postagens no blog da OIC do Reino Unido sobre os mitos acerca do RGPD.

8 Veja também as diretrizes do WP29 (minuta) sobre o Consentimento ao abrigo do Regulamento 2016/679 (WP259) e as orientações da OIC sobre consentimento.

9 Diretrizes do WP29 sobre notificação de violação de dados pessoais ao abrigo do Regulamento 2016/679 (WP250rev.01).

10 Veja também a seção "Transferência de dados".

11 Consulte, por exemplo, a preparação da OIC do Reino Unido para o RGPD - 12 passos a serem tomados agora (PDF).

12 Consulte também a seção "Desmistificando o RGPD".

13 Consulte a seção "Recursos úteis sobre o RGPD".

14 Para mais informações sobre o Responsável de Privacidade Global e o Diretor de Segurança da Informação, consulte a seção Biografia.

15 Como parte do projeto de certificação pelo Escudo de Proteção da Privacidade UE-EUA, já incluímos as cláusulas contratuais necessárias do RGPD em muitos dos contratos com nossos fornecedores (subprocessadores) que têm acesso às informações pessoais da UE.

16 Lembramos que nem todos os requisitos de produto se aplicam a todos os produtos. Por exemplo, alguns produtos não possuem uma interface de usuário que permita que os clientes vinculem-se a suas políticas/notificações de privacidade.

17 Consulte a seção "Segurança" para maiores detalhes.

18 Uma vez que uma rede ou sistema esteja conectado à internet, a localização física dos dados tem pouco ou nenhum impacto sobre as ameaças à segurança. Consulte o artigo da Amazon Web Services (AWS) "Data Residency AWS Policy Perspective" (em particular as páginas 2 e 3) para obter argumentos convincentes contra a localização de dados.

19 Na data deste documento.

20 Consulte os Programas de Conformidade da AWS para obter a lista completa de certificações e conformidade legal.

21 Art. 28(2)-(4) RGPD.

22 Art. 33 e 34 RGPD.

23 Para uma explicação sobre o papel do processador de dados, consulte a seção "O papel de nossa e de sua organização sob o RGPD".

24 Consulte a seção "Desmistificando o RGPD" acima para obter mais detalhes sobre o momento e o processo de notificação de violação de dados pessoais.

25 Veja também a seção "Contratos com clientes".