PLANO DE AÇÃO PARA ADEQUAÇÃO À LGPD
YAMAHA Brasil | Omnisblue

Apresentação do projeto
O projeto associado a este documento trata da realização de ***atividades de assessoria visando a implementação de programa de adequação a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018) para a unidade P&PD - Privacidade e Segurança de Dados da Yamaha Brasil.***

Objetivos do documento
- Documentar o resultado obtido após conclusão da etapa de **Preparação** / **Diagnóstico** do projeto de adequação à LGPD em execução na **Yamaha**;
- Direcionar os times da **Yamaha** em relação às atividades que precisam ser concluídas para finalizar a etapa de **Engajamento** / **Adequação** do projeto.

Fundamentos legais
As análises e definições presentes neste documento estão fundamentadas na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18), nos parâmetros definidos pela norma ISO/IEC 27.001 e pelas estratégias definidas no framework de adequação à LGPD de propriedade da Omnisblue.

Todas as ações sugeridas aqui têm como origem as informações fornecidas pelo Controlador durante a etapa de Preparação / Diagnóstico da Adequação à LGPD e essas informações estão todas inventariadas no ambiente *Privacy & Compliance Project (PCP)* do Controlador.

É imperativo que o Controlador e seus representantes tomem ciência das informações presentes na plataforma de governança de privacidade implementada (PCP) e, em caso de distorção em relação à realidade operacional de suas rotinas, alerte a Omnisblue, uma vez que as informações ali contidas foram fruto de levantamento e narrativas apresentadas pelos próprios representantes do Controlador.

Resumo do projeto
O projeto de adequação à LGPD se iniciou com a elaboração do *Plano de Projeto* conhecido e firmado entre as partes e teve sua primeira ação mais palpável observável por todos os *Stakeholders* com a reunião de kick off do projeto.

A partir do alinhamento entre as partes, foram realizadas diversas atividades de levantamento entre o time de especialistas da Omnisblue e os colaboradores do cliente (internos ou terceiros) onde foram levantados os aspectos *operacionais, tecnológicos* e *jurídicos* do Controlador relacionado à unidade P&PD.

Esses levantamentos detalharam o escopo do projeto de acordo com os seguintes quantitativos inventariados:

- **40 processos de negócio**
  - Negócio 33
  - LGPD 6
  - Gestão de Medidas Administrativas 1

- **23 ativos de informação**
- **83 artefatos contendo o uso de dados pessoais**
- **65 metadados pessoais em uso**
- **92 rotinas de tratamento de dados pessoais**
- **32 medidas administrativas de segurança (políticas)**
- **13 terceiros envolvidos nas rotinas de tratamentos de dados e/ou gestão de ativos de informação**
- **13 riscos de segurança e privacidade**
  - Estratégicos 01
  - Operacionais 12
- **07 atividades de adequação a serem executadas nas etapas de Engajamento e Adequação**
  - Aspectos operacionais e administrativos 03
  - Aspectos tecnológicos 04

Todas as informações inventariadas, e disponibilizadas no ambiente de produção do *Privacy & Compliance Project (PCP)*, foram na sequência analisadas pelos especialistas da Omnisblue e, a partir dessa análise, foram elencados os *Riscos de Privacidade e Proteção de Dados Pessoais* associados ao escopo tratado no projeto e, a partir desses riscos, foram definidas as *Atividades de adequação* pendentes de execução para completar o ciclo de adequação do Controlador à Lei Geral de Proteção de Dados dentro dos limites de escopo do projeto.

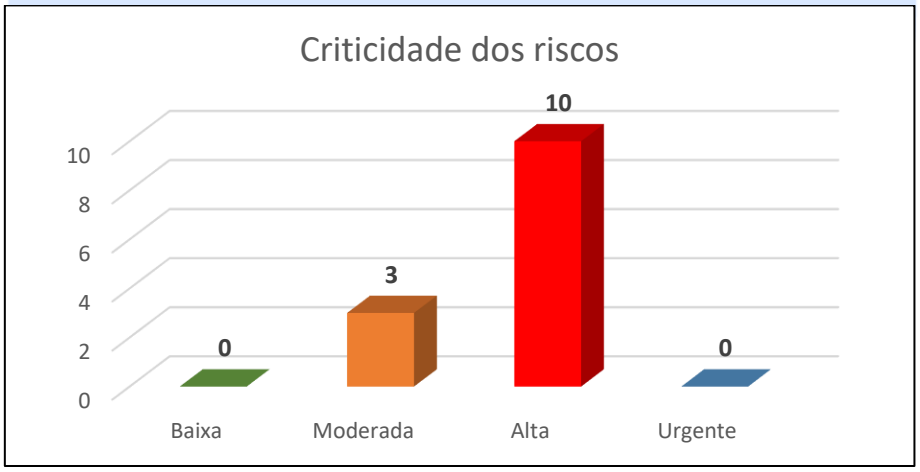
A seguir detalhamos então os *Riscos* e as *Atividades* definidas que endereçam as etapas de **Engajamento** / **Adequação** que passam a ser executadas a partir da aprovação deste documento.

Visão geral dos riscos de privacidade e proteção de dados

Os riscos encontrados, inventariados e com suas respectivas estratégias definidas foram classificados de acordo com sua criticidade que é automaticamente observada de acordo com a seguinte matriz de classificação de impacto *versus* probabilidade:

Probabilidade	Impacto: Baixo	Impacto: Médio	Impacto: Alto
100%	Alta	Urgente	Urgente
90%	Moderada	Urgente	Urgente
80%	Moderada	Alta	Urgente
70%	Moderada	Alta	Urgente
60%	Moderada	Alta	Alta
50%	Baixa	Alta	Alta
40%	Baixa	Moderada	Alta
30%	Baixa	Moderada	Moderada
20%	Baixa	Baixa	Moderada
10%	Baixa	Baixa	Moderada

Esses riscos podem ser analisados em detalhe no ambiente PCP do Controlador, na funcionalidade "Riscos" e a distribuição de suas respectivas criticidades pode ser compreendida de acordo com o gráfico a seguir:



As atividades de adequação detalhadas a seguir tratam, inclusive, das ações a serem realizadas para executar as estratégias de gestão e monitoramento de todos os riscos inventariados pelo projeto até o momento.

A lista de riscos de privacidade deve ser compreendida como uma entidade que evolui ao longo do tempo, onde novos riscos serão descobertos, encerrados, disparados ou terão seus atributos modificados de acordo com eventos internos ou externos ao Controlador. A gestão desses riscos, muito além das atividades definidas neste plano, deve ser tarefa contínua, a ser realizada pelo DPO do Controlador durante a fase de **Operação** do ciclo de vida do Sistema de Gestão de Privacidade e Proteção de Dados (SGPD).

Visão geral das ações de adequação a serem realizadas

As análises sobre todas as informações inventariadas durante a etapa de **Preparação** / **Diagnóstico** geraram uma lista de ações / atividades a serem executadas a seguir no projeto. Essas atividades foram cadastradas no ambiente PCP do Controlador na funcionalidade "Atividades e Ações".

Essas atividades podem ser classificadas de acordo com os aspectos de sua natureza técnica predominante, tal como segue:

- **Aspectos operacionais e administrativos:** Tratam de ações que alteram rotinas operacionais e administrativas do Controlador, adequando aspectos geralmente mais associados a papéis e responsabilidades, medidas administrativas e fluxo de informação e processos;
- **Aspectos tecnológicos:** Tratam de ações que alteram requisitos de Tecnologia da Informação do Controlador, adequando aspectos geralmente mais associados parâmetros de TI de Ativos de Informação eletrônicos e medidas técnicas de segurança;
- **Aspectos jurídicos:** Tratam de ações que alteram parâmetros jurídicos, legais e/ou contratuais do Controlador, adequando aspectos geralmente mais associados a contratos, bases legais, autorizações e responsabilidades legais;
- **Aspectos evolutivos:** Tratam de sugestões para se expandir a abrangência do SGPD em implantação para outras áreas ou departamentos do Controlador, bem como detalhar ainda mais as rotinas operacionais em busca de informações que porventura não foram detectadas durante as rotinas de levantamento realizadas pelo projeto até aqui.

A seguir listamos todas as atividades levantadas e planejadas, agrupadas de acordo com sua classificação de seus aspectos conforme definidos acima utilizando o seguinte padrão:

[XXXXXXXX] – XXXXXXXXXXXXXXX [XXXXXXX]

Tipo da atividade (imediata ou contínua)	**Descrição da atividade** (conforme inventariado no PCP)	**Responsável principal** pela ação

O tipo da atividade define se a sugestão para a execução da ação é **imediata** (*a ser executada pela parte responsável ainda dentro do prazo e escopo do projeto atual*) ou se é **contínua** (*a ser executada pelo DPO do Controlador em etapas complementares / futuras de gestão do SGPD*).

Aspectos operacionais e administrativos (03)

As atividades mais associadas aos aspectos operacionais e administrativos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Imediata] - [P&PD] - Implementar/ajustar as rotinas de descarte de dados pessoais eletrônicos na unidade/departamento [Júlio Cesar Torquato Dos Santos]**
  - *Descrição:* Fazendo uso da nova política de descartes de dados do controlador, compatibilizar as rotinas de exclusão e esquecimento de dados pessoais eletrônicos realizadas pela unidade/departamento de acordo com os requisitos pré-estabelecidos.

- **[Imediata] - [P&PD] - Implementar política de impressão na unidade/departamento [Júlio Cesar Torquato Dos Santos]**
  - *Descrição:* Fazendo uso da nova política de segurança do controlador, apresentar as regras de "compartilhamento de impressão" que devem ser observadas na unidade/departamento, garantindo segurança e disponibilidade ideal das informações físicas tratadas na área.
    Essas regras devem ser demonstradas aos colaboradores, bem como a obrigatoriedade de serem seguidas, sob pena de sanções administrativas.

- **[Imediata] - [P&PD] - Implementar política de retirada de documentos físicos das dependências do controlador [Júlio Cesar Torquato Dos Santos]**
  - *Descrição:* Fazendo uso da nova política de segurança do controlador, apresentar as regras de uso de documentos físicos fora do ambiente de trabalho, proibindo a retirada de documentos físicos do ambiente para fora das dependências do controlador sem devido uso de Termo de Responsabilidade. Essas regras devem ser observadas na unidade/departamento, garantindo segurança e disponibilidade ideal das informações físicas tratadas na área.
    Essas regras devem ser demonstradas aos colaboradores, bem como a obrigatoriedade de serem seguidas, sob pena de sanções administrativas.

Aspectos tecnológicos (04)

As atividades mais associadas aos aspectos técnicos e tecnológicos de adequação à LGPD que devem ser executadas para completar a adequação do Controlador dentro dos limites do projeto em questão são:

- **[Imediata] - [P&PD] - Implementar criptografia de discos nos dispositivos corporativos [Júlio Cesar Torquato Dos Santos]**
  - *Descrição:* Os dispositivos utilizados para acessar os ativos de informação eletrônicos em uso na unidade/departamento (desktops e notebooks) devem ser configurados de forma que seus discos possuam criptografia ativada, garantindo que apenas usuários com senhas possam acessar o conteúdo de seus discos.
    Para equipamentos Windows, utilizar, por exemplo, o BitLocker.

- **[Imediata] - [P&PD] - Implementar medidas técnicas de criptografia nos dispositivos pessoais [Júlio Cesar Torquato Dos Santos]**
  - *Descrição:* Os dispositivos pessoais dos colaboradores da unidade/departamento, utilizados para a realização de atividades de trabalho, devem estar configurados com as medidas técnicas de criptografia, garantindo que acessos indevidos não realizem o compartilhamento de dados pessoais com pessoas não autorizadas.

- **[Imediata] - [P&PD] - Implementar acesso remoto por VPN nos ativos eletrônicos da unidade/departamento [Júlio Cesar Torquato Dos Santos]**

- *Descrição:* O acesso remoto aos ativos de informação eletrônicos em uso na unidade/departamento deve ocorrer apenas utilizando-se uma conexão via VPN, mitigando riscos de acesso indevido às informações em tratamento.

- **[Imediata] - [P&PD] - Implementar monitoramento de câmeras nos ambientes onde são armazenados os ativos físicos [Júlio Cesar Torquato Dos Santos]**
  - *Descrição:* Os documentos (artefatos) físicos em uso na unidade/departamento devem ser armazenados em local seguro, com monitoramento de câmera que garanta a possibilidade de se consultar histórico de acesso ao local.
    Sugere-se que as imagens sejam armazenadas por um período de ao menos 30 (trinta) dias, e descartadas/substituídas após esse período.

Conclusão

As ações sugeridas neste Plano de Ação já foram cadastradas no PCP para controle e acompanhamento de seus resultados e, este documento deve ser conhecido por todos os *Stakeholders* do Controlador que porventura sejam envolvidos direta ou indiretamente na execução dessas ações.

Os prazos, as datas planejadas para a execução de cada atividade prevista neste Plano de Ação e eventuais interdependências entre as atividades são aspectos que estão detalhados no *Cronograma do projeto* que deve ser atualizado considerando os detalhes aqui definidos.