# A Arquitetura Corporativa e a Proteção de Dados Pessoais

Marc Lankhorst, Razvan Mitache
& Antonio Plais

V2.0

# Conteúdo

# Introdução

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709 de 2018), sancionada pelo Presidente Michel Temer em agosto de 2018, foi fortemente inspirada pelo General Data Protection Regulation (GDPR), elaborado no âmbito da União Europeia. A LGPD pretende transformar completamente a forma como as organizações lidam com os dados pessoais de seus clientes e, por consequência, a própria forma como elas se relacionam com eles. Ela consolida, reforça e cria vários deveres e direitos, muitos deles já presentes em outros marcos legais, como o Marco Civil da Internet, o Código de Defesa do Consumidor e a Lei do Cadastro Positivo, e, principalmente, fornece as bases legais para um relacionamento mais equilibrado entre as empresas que processam e armazenam dados pessoais e os indivíduos que são, em última instância, os legítimos proprietários de seus próprios dados.

Com entrada em vigor pleno prevista inicialmente para fevereiro de 2020, e adiada para agosto do mesmo ano, a LGPD força as empresas a reverem boa parte de seus processos, sistemas e políticas de coleta, tratamento, armazenamento e utilização de dados pessoais e sensíveis, impactando, inclusive, em vários modelos de negócio comumente utilizados no mercado. Em resumo, a LGPD baseia o tratamento legítimo dos dados pessoais nos seguintes princípios (Artigo 6°):

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

- Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas;

A LGPD estabelece uma série de obrigações para as empresas, e aquelas que não cumprirem as diretivas estabelecidas poderão sofrer pesadas sanções, como multas simples ou diárias de até 2% do faturamento líquido do último ano, limitado a R$50 milhões, POR INFRAÇÃO, além de outras penalidades. Depois de muitas discussões e idas e vindas no Congresso, e devido ao enorme atraso na implantação da Agência Nacional de Proteção de Dados (ANPD), responsável pela regulamentação de vários pontos da Lei e pela aplicação das sanções, a LGPD entrou finalmente em vigor em agosto de 2020, com início da aplicação das penalidades postergada para agosto de 2021.

É importante frisar, no entanto, que a falta de instalação efetiva da ANPD não impede que outras esferas administrativas e judiciais usem os requisitos da LGPD para motivar sanções contra empresas que não se conformarem com as suas diretivas, de forma que, apesar de tumultuado, podemos afirmar que o espírito de proteção dos dados pessoais veio definitivamente para ficar, e só resta às empresas se enquadrarem e ajustarem seus processos, sistemas e políticas ao que a LGPD exige.

Os arquitetos corporativos podem ter um importante papel para auxiliar suas organizações a se tornarem conformes com a LGPD. Nas páginas a seguir, veremos o que a conformidade com a LGPD envolve, o impacto que ela tem sobre a sua organização, e exploraremos maneiras como os arquitetos podem lidar efetivamente com os seus requisitos e restrições.

# Principais Percepções sobre a LGPD

Para começar, aqui estão sete percepções importantes que você deveria saber sobre a LGPD:

## A LGPD se aplica a todas as empresas que processam dados de indivíduos no Brasil

Mesmo que a empresa não esteja localizada no Brasil, a LGPD pode ser aplicável a ela. Como declarado no Artigo 3, ela "se aplica a qualquer operação de tratamento ... realizada em território nacional; .... destinado à oferta de serviços e produtos ... para indivíduos localizados no território nacional; .... ou cujos dados tenham sido coletados no território nacional". Isso implica que, com algumas exceções previstas na Lei, praticamente qualquer empresa que processe dados pessoais de indivíduos no Brasil está sujeita às suas normas, requisitos e penalidades.

## A LGPD tem a ver com demonstrar a conformidade

Além de estar em conformidade, você também deve demonstrar conformidade. O Artigo 6, Inciso X, declara: "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Os arquitetos corporativos estão particularmente bem-posicionados para ajudar suas organizações a demonstrar que elas estão conformes. Alavancando seus modelos de arquitetura para propósitos de privacidade e segurança, os arquitetos podem fornecer análises transversais sobre o uso e a proteção dos dados através da empresa, seus processos, pessoas e sistemas de TI.

## A LGPD espera que você registre o propósito da coleta de dados pessoais

Você deve registrar o que você faz com os dados pessoais e para qual propósito (Artigo 37). Isso inclui coisas como: *Em quais locais os dados pessoais são armazenados? Quais aplicativos os utilizam? Quem tem acesso a esses aplicativos? Com quais terceiros fazemos compartilhamento? Onde eles estão localizados?* etc. Procedimentos de conformidade existentes muitas vezes tentam capturar isso usando planilhas e outros documentos do tipo Office, mas isso rapidamente se torna impossível de gerenciar. Os arquitetos podem desempenhar um papel fundamental na simplificação de procedimentos, uma vez que seus modelos de arquitetura geralmente contêm muito do que é necessário para obter essa visão geral integrada do uso de dados.

## A LGPD exige uma abordagem integrada de segurança por desenho

Você deve implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, o que inclui um processo para testar e avaliar regularmente a eficácia dessas medidas. Simplesmente acrescentar algumas poucas medidas de segurança depois que o sistema entrar em operação não fará isso. Isso requer uma abordagem integrada para segurança por desenho, não se concentrando apenas na parte da TI, mas englobando todos os aspectos de sua organização. Arquitetos corporativos estão bem-posicionados para lidar com isto, uma vez que eles possuem a visão geral e a percepção necessária para isso.

## A LGPD requer Relatório de Impacto da Proteção de Dados

Você deve fornecer um Relatório de Impacto da Proteção de Dados quando solicitado pela Autoridade Nacional de Proteção de Dados (ANPD), o que inclui os tipos de dados coletados e métodos de coleta, uma descrição sistemática do processamento, a avaliação dos riscos à segurança das informações e as medidas para mitigar estes riscos. Uma análise como esta, em panoramas de TI e de negócios grandes e complicados, requer soluções de software inteligentes. A funcionalidade de Gerenciamento de Segurança, Risco e Conformidade do BiZZdesign Enterprise Studio é perfeitamente adequada para este tipo de análise e desenho de privacidade e segurança. Alavancar seus modelos de arquitetura existentes lhe dá um ótimo pontapé inicial!

### A LGPD determina que você denuncie incidentes de segurança

Você deve relatar incidentes de segurança de dados pessoais à ANPD e aos titulares envolvidos em "prazo razoável" a ser definido pela ANPD (Artigo 48), com possível comunicação ampla e pública do evento. Isso representa sérios riscos à reputação, como incidentes anteriores de grande repercussão no mercado têm demostrado. Tentar esconder uma violação não é mais uma opção.

### A LGPD pode levar a penalidades significativas

As penalidades por não-cumprimento incluem "multa de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração" (Artigo 52), além de danos pessoais que podem ser reclamados por titulares de dados (também por meio de ações coletivas) e eventuais ações civis e criminais. Tal impacto financeiro seria suficiente para pôr em perigo a existência de muitas empresas. Qual seria o valor para sua organização evitar esses riscos?

## Por que a Arquitetura é Importante?

A segurança cibernética e os riscos de reputação associados se tornaram uma das principais preocupações estratégicas para a alta direção, e a LGPD torna este problema mais relevante do que nunca. Para garantir que a sua organização está conforme, você precisa de uma visão geral ampla sobre como os dados pessoais são usados e porque eles são coletados, como eles são processados, quem tem acesso a eles, onde eles são armazenados, quais terceiros estão envolvidos, que ameaças internas e externas existem, e muito mais. Como um arquiteto corporativo, você possui uma visão abrangente e integrada única da sua organização, bem como os modelos e as ferramentas necessárias para avaliar, melhorar e garantir a proteção dos dados.

Isso é ainda mais verdadeiro quando você considera - e já mencionamos isso acima - que a LGPD exige não apenas a conformidade, mas também a capacidade de comprovar a conformidade. A arquitetura e os modelos da arquitetura (deveriam) se destacam naturalmente como a maior fonte desta informação, em particular quando você precisa de uma visão conectada e coerente de tudo o que está relacionado com dados pessoais.

Tudo isso significa que você pode e deveria desempenhar um papel fundamental para ajudar sua empresa a superar os desafios da LGPD. Descubra o valor oculto de seu conhecimento, modelos e análises de arquitetura, e ajude a empresa a melhorar sua resiliência cibernética, garantir a conformidade normativa e reduzir os riscos operacionais, de reputação e financeiros.

# Passos a Dar como um Arquiteto

Vamos ver alguns passos que você pode dar para ajudar a sua organização a se conformar com a LGPD.

## Trabalhe em Equipe com as Partes Interessadas Certas

Na maioria das organizações, os arquitetos corporativos não têm a responsabilidade final por garantir a conformidade regulatória. Esta responsabilidade pode estar nas mãos de seu Departamento Jurídico, Diretor de Riscos, Diretor de Conformidade, Diretor de Segurança da Informação, ou com o novo Encarregado de Proteção de Dados, requerido pela LGPD. Se aproximar destes executivos, e fazer com que eles se conscientizem da contribuição valiosa que a arquitetura pode trazer, é o primeiro passo.

## Crie um Inventário de Privacidade

Criar um "inventário de privacidade" é crucial, uma vez que qualquer trabalho para garantir a conformidade dependerá de uma boa visão geral dos dados pessoais envolvidos (veja a Figura 1). Aqui está o que você deveria ter em mente:

a. Identifique todos os dados considerados 'pessoais' de acordo com a LGPD.
b. Classifique estes dados em relação à sua sensibilidade à privacidade. Torne isso parte do seu processo normal de segurança, onde você atribui outros atributos de segurança da informação (tais como, confidencialidade, integridade e disponibilidade) aos seus dados.
c. Descreva o propósito para o qual estes dados foram coletados, e garanta que você tem (ou obtenha) o consenso dos sujeitos de dados (as pessoas!) para usá-los desta forma.
d. Preste atenção adicional às categorias especiais de dados pessoais, tais como dados relacionados à saúde, biométricos, políticos, religiosos, étnicos ou associação sindical. O uso destes dados é explicitamente restringido pela LGPD, a não ser que circunstâncias especiais muito específicas se apliquem.

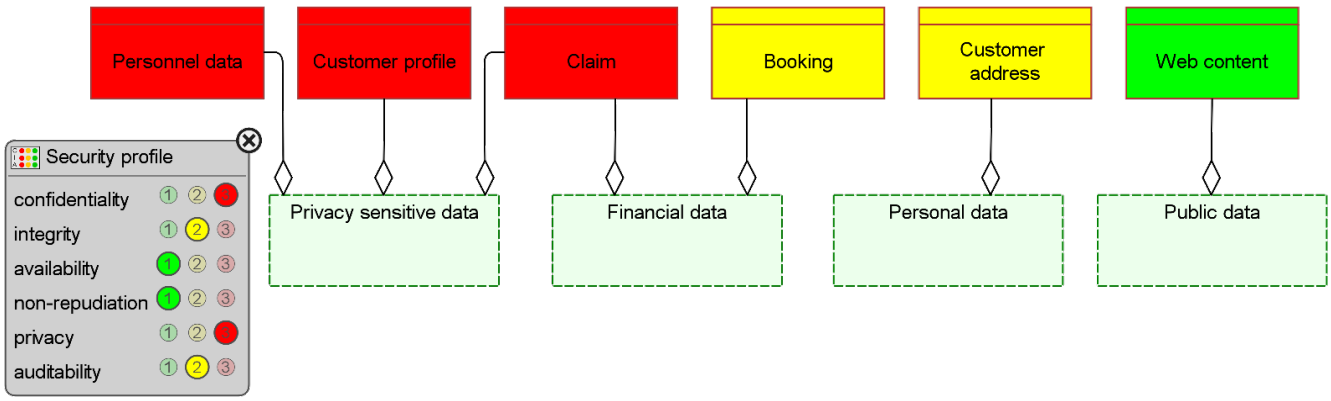


*Figura 1: Classificação de dados com cores com base na sensibilidade à privacidade*

## Avalie o Uso dos Dados Pessoais

Você deveria analisar o uso dos dados pessoais e, se possível, alavancar seus modelos de arquitetura existentes para fornecer uma estrutura para suas análises (veja a Figura 2). Aqui estão algumas ideias:

a. Comece com as áreas de alto risco e com os tipos de dados mais sensíveis. Onde eles são armazenados e usados?
b. Modele os fluxos de dados: quais aplicativos, processos, pessoas e parceiros usam estes dados, em quais locais, para qual propósito?

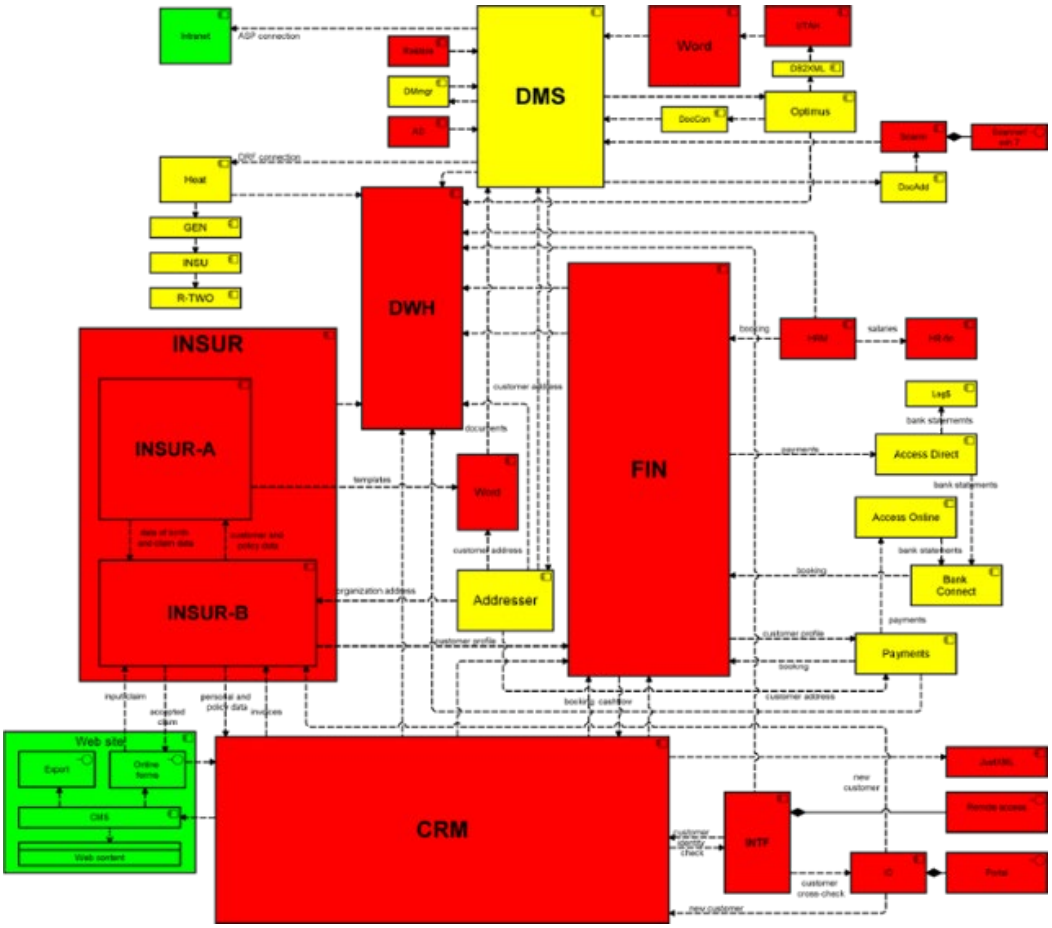


*Figura 2: Panorama de aplicativos com cores baseadas na classificação de privacidade dos dados usados*

## Avalie os Riscos para os Dados Sensíveis

Avalie os riscos para os dados sensíveis, em particular em relação aos direitos e liberdades dos sujeitos de dados. Considere o seguinte:

a. Onde você vê vulnerabilidades no seu panorama de TI e de negócios?
b. Quais são algumas ameaças comuns que podem explorar estas vulnerabilidades?
c. Quais são as possíveis consequências?

Você pode usar a funcionalidade de Gerenciamento de Segurança, Risco e Conformidade do BiZZdesign Enterprise Studio para fazer análises avançadas dos riscos, com base nos padrões ArchiMate e Open FAIR, do The Open Group. Os mapas de calor mostrados na Figura 3 são um exemplo do tipo de saída que pode ser criada. A Centus-BiZZdesign pode fornecer para seus clientes conteúdo pré-populado contendo informação útil sobre ameaças de segurança e de continuidade do negócio, e os objetivos e controles prescritos por vários padrões de segurança. Isso lhe dá um bom ponto de partida, pois ajuda a evitar que você reinvente a roda.

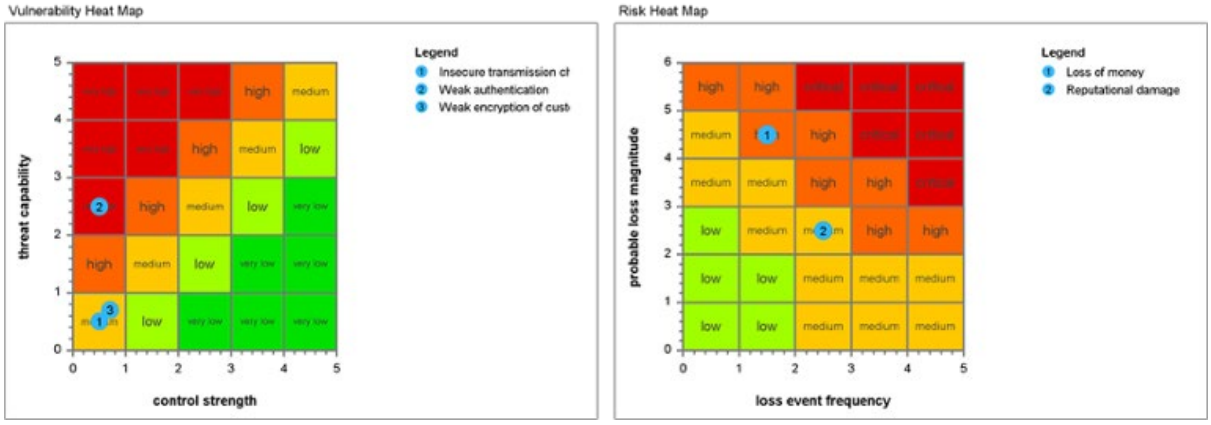


*Figura 3: Mapas de calor de avaliação de riscos*

## Defina Controles

Defina os controles e medidas mitigadoras. Use padrões comuns, como o ISO/IEC 27001, como a base para identificar controles úteis. Mais importante, você deveria fazer isto o mais cedo possível durante o processo de desenho ou mudança de seus sistemas, para promover uma abordagem de proteção de dados por desenho e evitar a incorporação destas medidas em um estágio posterior, com todo o retrabalho, custo e risco associados.

## Priorize os Riscos

Priorize os riscos, aloque os orçamentos e planeje os requisitos para as mudanças e melhorias. Aqui estão algumas ideias:

a. Avalie os custos das medidas contra os riscos (a perda esperada) para focar seu orçamento naquilo que realmente conta.
b. Integre esta tomada de decisão com o gerenciamento geral do portfólio e com os roteiros. Por exemplo, você deve evitar gastar muito em manter um aplicativo que será desativado em pouco tempo, e você deve combinar melhorias relacionadas com a segurança com outras mudanças.

A funcionalidade de Gerenciamento de Portfólios do Enterprise Studio também é muito útil neste estágio Painéis de controle claros ajudam a gerência a decidir sobre as prioridades e investimentos, levando todos os ângulos de avaliação em consideração, e permitindo que você filtre e foque naquilo que é essencial, como mostrado na Figura 4 abaixo:

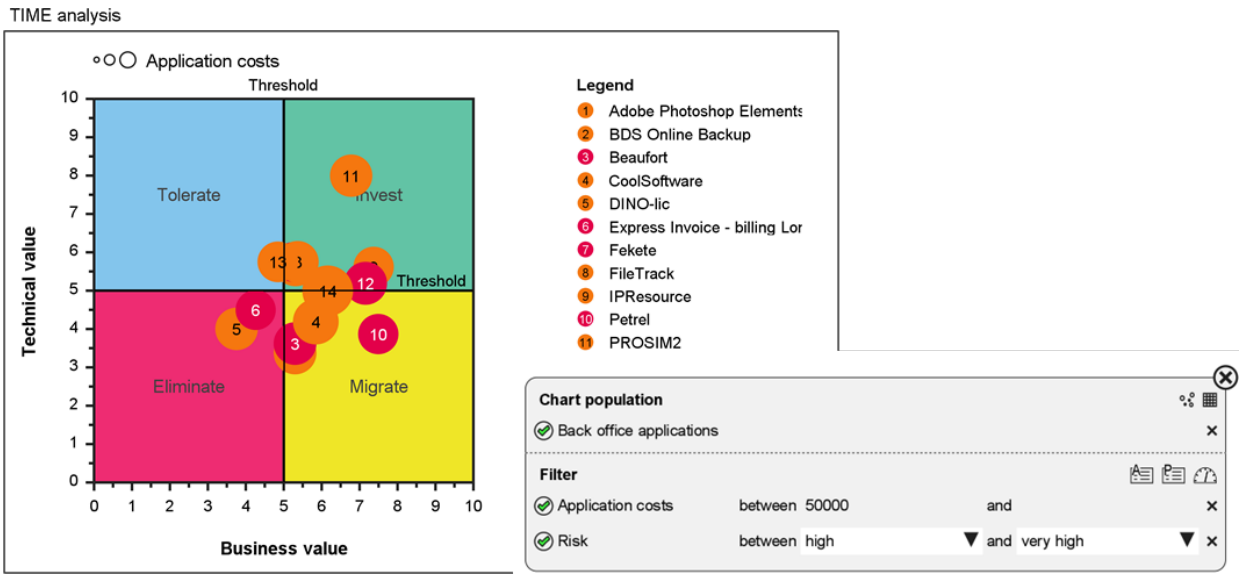


*Figura 4: Gráfico do ciclo de vida do portfólio de aplicativos filtrado para aplicativos de alto risco e alto custo*

## Implemente e Teste as Medidas

Você deveria implementar e testar os controles e medidas que você definiu para a sua organização, processos e sistemas, e avaliar o seu nível de segurança. É claro que isso é o que mais importa!

## Demonstre a Conformidade

Quando necessário, demonstre a conformidade para as autoridades reguladoras, mostrando como você processa os dados pessoais, como você lida com os riscos, e quais medidas mitigadoras você implementou. Lembre-se, seus controles não ajudarão muito se você não puder tornar seu progresso visível para o regulador.

Naturalmente, esta não é uma abordagem a ser realizada uma única vez. Você deveria revisitar os passos acima para garantir que você continua conforme e integrar isto no seu framework de governança. Estes passos são também particularmente relevantes quando você avalia seu Relatório de Impacto da Proteção de Dados, que deveria ser realizado para qualquer implementação de um novo sistema ou alteração em sistemas existentes que processem dados pessoais.

## Criação de Registros da LGPD no Enterprise Studio

Nós já cobrimos a rigorosa natureza da LGPD no início deste artigo. Alguns daqueles problemas afetarão principalmente seus processos (de desenho) - pontos 4, 5 e 6 - enquanto outros terão mais impacto sobre o que e como você registra os dados pessoais, bem como onde e como você processa esses dados - pontos 1, 2 e 3. Como muitas organizações terão dificuldades em implementar e cumprir a LGPD, certamente uma solução prática que aborde algumas das questões mencionadas acima seria bem-vinda.

As empresas precisam criar e manter registros do porquê, onde e como estão processando dados pessoais. Criar e manter esses registros no BiZZdesign Enterprise Studio ajuda a garantir que você crie registros consistentes e coerentes que estejam em conformidade com o desenho atual da sua empresa. Um registro desse tipo pode ser algo tão simples quanto uma planilha, desde que todos os dados necessários estejam contidos dentro dela. Aqui está um exemplo de uma lista de itens relevantes:

- Nome das atividades de processamento
- Motivo para o processamento dos dados
- Base legal para o processamento
- Explicação
- Quem está envolvido (internamente)?
- Quem é responsável internamente?
- Quem é responsabilizável?
- Quais dados são processados
- Categorias especiais de dados
- Origem dos dados
- Categorias de partes receptoras
- Outros terceiros que recebem dados
- Período de retenção
- Contrato de processamento
- Tipo de processamento
- Aplicativos envolvidos
- Avaliação de impacto na privacidade necessária

É claro que é possível optar por ter esse registro disponível somente internamente e criar um registro disponível publicamente que contenha menos itens. Você pode usar o Enterprise Studio para dar suporte a este caso de uso específico da LGPD: criar e manter registros de dados pessoais. Para começar, para criar e manter essas informações recomendamos que você não crie um registro separado, mas integre as informações necessárias aos modelos de arquitetura atuais no Enterprise Studio. Em geral, você deve executar as seguintes etapas no Enterprise Studio (consulte também a Figura 5 abaixo):

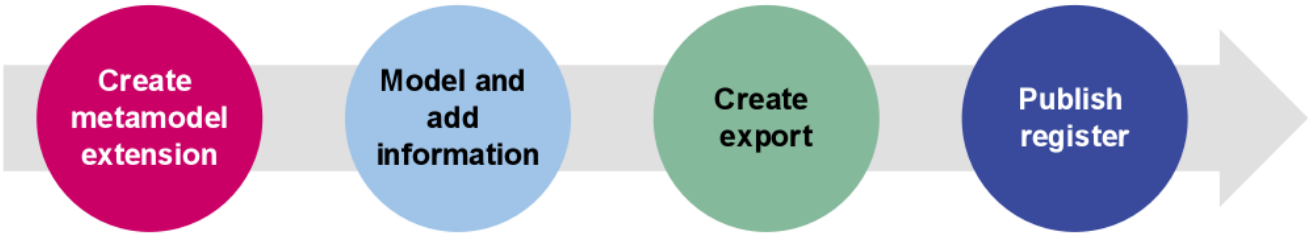


*Figura 5: Visão geral das etapas*

## Criar uma extensão do metamodelo

Personalize o metamodelo no Enterprise Studio para incluir os atributos mencionados acima (ou outros que você julgue necessários). Optamos por adicionar um perfil especial com os atributos necessários ao conceito Processo de Aplicativo do ArchiMate. Além disso, criamos estereótipos para Objetos de Dados e Atores de Negócio para distinguir categorias de dados, dados especiais e terceiros. Depois de aplicar o metamodelo, o perfil seria semelhante ao da Figura 6.

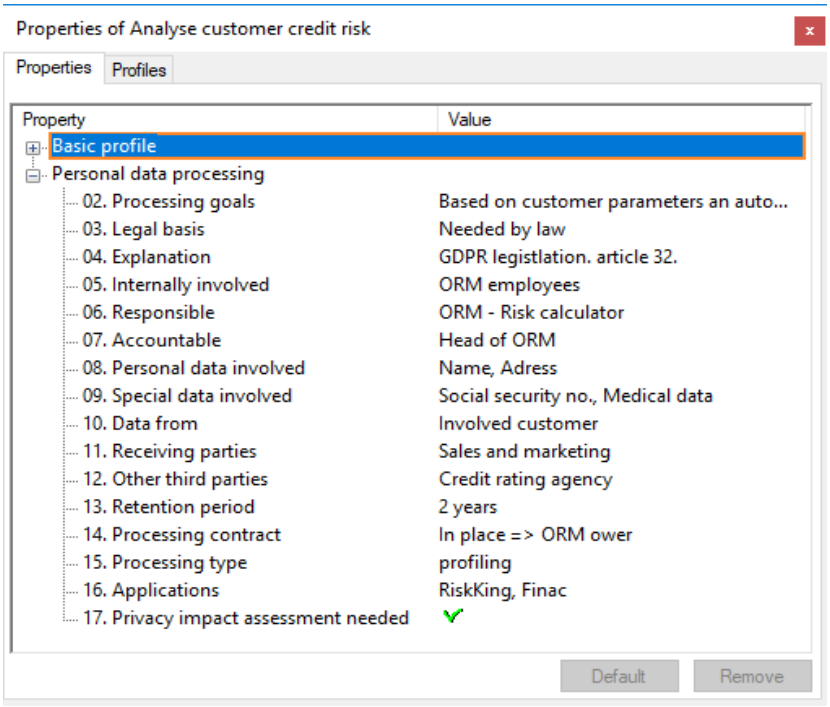


*Figura 6: Exemplo de perfil*

## Modelar e adicionar os dados

Reunir todas as informações sobre o processamento de dados pessoais em sua empresa é a parte mais difícil. Talvez você possa aproveitar as avaliações que já foram feitas. Na Figura 7, você vê um exemplo de modelo de um cenário de processamento de dados.

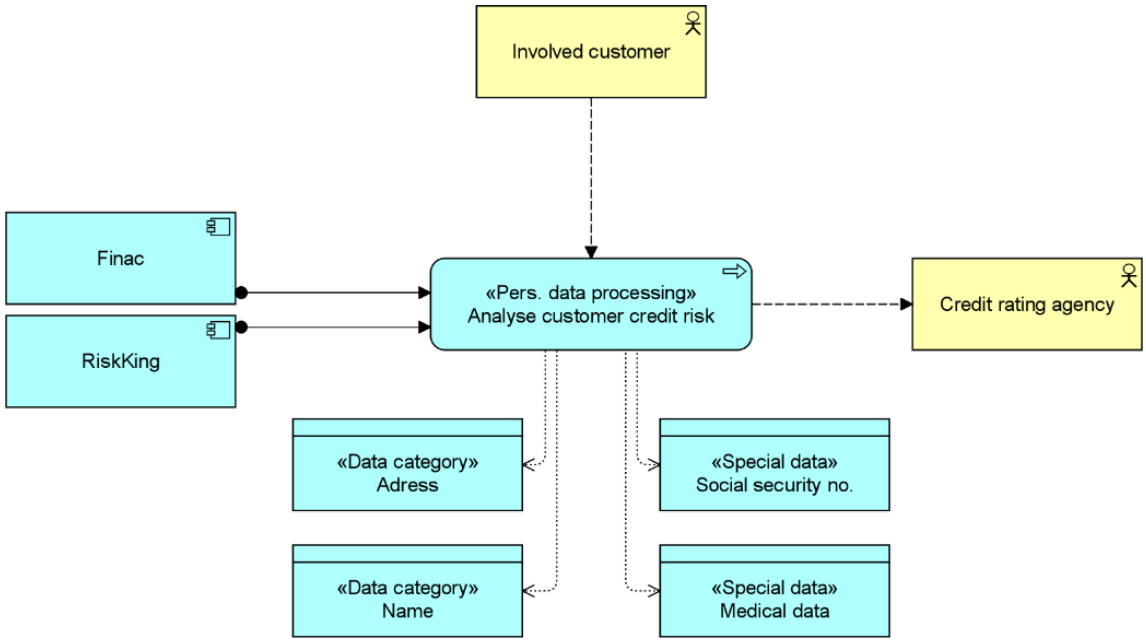


*Figura 7: Cenário de processamento de dados*

## Criar uma exportação

Use a poderosa funcionalidade de exportação do Enterprise Studio para exportar os dados para uma planilha do Excel (Figura 8). Você pode optar por desenvolver dois tipos de exportação, um com o registro completo e outro com as informações disponíveis publicamente.

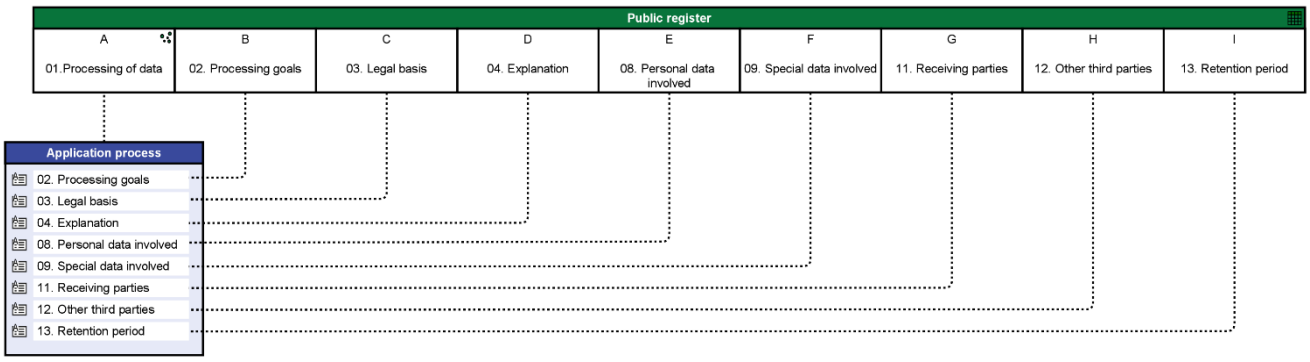


*Figura 8: Exportando os dados para uma planilha do Excel*

## Publicar o registro

Agora você pode publicar seu(s) registro(s). Se você tiver implementado um processo de mudança adequado, só precisará atualizar seu modelo e publicar um registro atualizado de vez em quando. As melhores práticas são realmente algo!

## Conclusão

Esperamos que tenhamos esclarecido um pouco o assunto do atendimento dos requisitos da LGPD e dado a você algumas boas percepções sobre como você pode ajudar sua organização a navegar pelo complexo mundo da conformidade com a LGPD, com a ajuda dos entregáveis da arquitetura corporativa. Um exemplo que esperamos tenha sido útil - adicionar dados da LGPD a modelos existentes e aproveitá-los para criar os registros necessários de processamento de dados pessoais - foi ilustrado acima com a ajuda do Enterprise Studio.

Se quiser saber mais sobre como a nossa plataforma pode ajudá-lo a lidar com a LGPD em particular ou com a conformidade regulatória em geral, entre em contato hoje mesmo ou solicite uma demonstração ao vivo gratuita!

## Sobre a BiZZdesign

A BiZZdesign é uma fornecedora líder de software e serviços de transformação empresarial baseada na Holanda. Fundada em 2000, como uma cisão comercial de um instituto de P&D, hoje a empresa possui presença global e é reconhecida pelos analistas de mercado como um líder de mercado. O principal produto da BiZZdesign, o Enterprise Studio, é utilizado pelas maiores empresas mundiais e organizações governamentais através dos cinco continentes, onde ele desempenha um papel fundamental na habilitação exitosa da mudança dos negócios.

## Sobre a Centus

A Centus é uma empresa de consultoria de negócios e transformação empresarial baseada em Belo Horizonte. Fundada em 2013, a empresa é focada na disseminação de conhecimentos sobre arquitetura corporativa, gerenciamento de decisões, transformação de negócios e a linguagem ArchiMate. Nossos principais produtos são plataformas de gerenciamento de decisões e de modelagem e repositório de arquitetura corporativa, contando com a parceria e o apoio de empresas líderes nos seus mercados, como a BiZZdesign.

Para mais informações, por favor visite bizzdesign.centus.com.br ou www.bizzdesign.com.