privIQ

LGDP
Guia de Onboarding

Índice

privIQ

LGDP
Onboarding Guide

Contents

Guia de Implementação

Se a sua organização atua como Controlador sugerimos que você adote a seguinte abordagem para implementar seu programa de conformidade com privacidade.

1. Entenda a atividade da organização perguntando:
    - Quais são as atividades principais?
    - Quantos empregados?
    - Você terceiriza o processamento de dados pessoais?
    - Você divulga dados pessoais para outras organizações?
    - Você transfere dados pessoais para fora do seu país ou região?
    - Quem chefia departamentos, por exemplo, RH, Vendas e outros que lidam com dados pessoais?
    - Quem está liderando o programa de privacidade?

2. Relacione os Chefes de departamentos (Proprietários das informações) para formular uma lista de todas as atividades de processamento que envolvem dados pessoais; incluindo as atividades informais. Registre as fontes dos dados pessoais, os aplicativos que processam dados pessoais, o local aonde as informações são armazenadas em seus departamentos e para quem as informações são divulgadas. Inclua as mídias físicas também.

3. Solicite dos Chefes de TI /Compras para compilar uma lista de todos os Fornecedores envolvidos com o processamento de dados pessoais, o país em que estão localizados, a data de validade desses contratos.

4. Informe o CEO / MD / chefe de organização do programa de proteção de dados.

5. Nomear o Oficial de Proteção de Dados, quando for o caso.

6. Registre-se na Autoridade Pertinente, quando necessário.

7. Certifique-se de que os parâmetros de configuração da organização estejam completos. (Veja a próxima seção).

8. Adicione os chefes de departamentos relevantes, o lead do programa, e usuários com função de administrador do sistema. Usuário de conformidade e proprietário de tarefas devem ser adicionados através das seções de Conformidade.

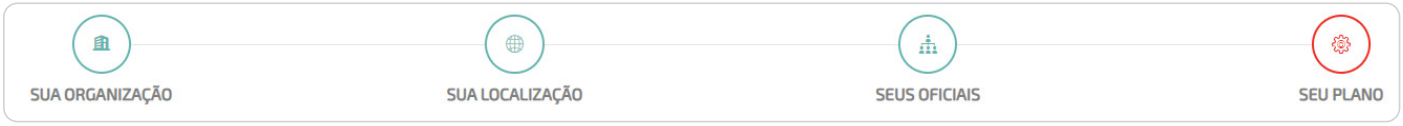
9. Adicione proprietários de informações para revisar e entender TODO o processamento de dados pessoais em seus respectivos departamentos. Registre também, todos os *processamentos informais*. Por exemplo: planilhas para gerenciar processos fora dos sistemas e aplicativos formais.

10. Inicie o mapeamento de dados, usando o trabalho de preparação feito pelos Proprietários das Informações.
    Defina datas para as entrevistas de mapeamento de dados.
    O Gerente de TI deve fornecer informações especialmente, sobre qualquer processamento de dados pessoais realizados por terceirizados (**operadores**).
    Use a sessão de acompanhamento para gerenciar o mapeamento de dados.

Siga as etapas indicadas pelas várias seções abaixo –
lembre-se, a conformidade está em andamento.

Configuração da organização

Para chegar às Configurações, clique na roda na barra de navegação superior.



Em **'Sua Organização'** insira seus dados de contato e faça o upload da logomarca.

Em **'Sua Localização'** digite seus endereços físicos e postais.

Em **'Seus Oficiais'** digite o nome e endereço de e-mail do líder da organização (por exemplo, o CEO), bem como os detalhes do DPO, quando disponível.

Em **'Seu Plano'** você encontrará as configurações e recursos que determinam o tamanho do seu pacote. Esteja ciente da troca entre mapeamento de dados por departamento. **Qualquer mapeamento de dados feito antes da troca de pacote será perdido.**

Termos-chave

Esses termos-chave são essenciais para a interpretação adequada do LGPD e para manter o aplicativo.

Controlador – pessoa física ou jurídica, de direito público ou privado, que tenha competência para tomar as decisões relativas ao tratamento de dados pessoais.

Operador – pessoa física ou jurídica, de direito público ou privado, que processa dados pessoais em nome do responsável pelo tratamento (controlador).

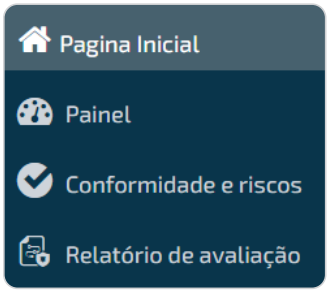
Dados Pessoais – informações sobre uma pessoa física identificada ou identificável.

Titular dos Dados – uma pessoa física a quem os dados pessoais objeto de processamento se referem.

Propietério da Informação – pessoa física que aprovou a responsabilidade gerencial pelo controle da manutenção, uso e segurança dos dados pessoais

Página inicial

Os recursos que você vê na página inicial serão aqueles que foram selecionados em Seu Plano, nas Configurações da Organização. Ao alternar entre diferentes seções, você é encorajado a usar a barra lateral.



Mapeamento de dados

Lembra-se daquele ditado sobre o RISCO – " Se você não pode medir, não pode gerenciar"
Se os Titulares solicitarem acesso aos seus dados pessoais, ou ocorrer um incidente de segurança, você precisa de um mapa detalhado para ajudá-lo a responder.
Mas o mapeamento de dados é muito mais do que produzir um inventário.

O Mapeamento de Dados representa o primeiro passo para construir uma base adequada que será utilizada para gerenciar seu programa de conformidade.
Registre informações sobre o processamento de dados pessoais: Quem? O quê? Por quê? Quando? Onde? Durante todo o processo, você pode adicionar seus próprios itens de dados, caso os itens padrão não sejam suficientes.

Os proprietários de informações devem direcionar o mapeamento de dados e estar envolvidos durante todo o processo. Identifique qualquer processamento informal e grave-o no mapeamento de dados. Estas são tipicamente as áreas de vulnerabilidade, e quaisquer riscos ou problemas relevantes, devem ser documentados e gerenciados na seção de conformidade

Antes de começar, entenda o significado de Granularidade

A granularidade é importante ao descrever seus propósitos de processamento. Pequenos detalhes devem ser incluídos nas informações, possibilitando um entendimento mais claro das atividades que envolvem processamento de dados.

Não utilize descrições genéricas para detalhar os tipos de processamento, especialmente quando envolvem diferentes tipos de dados pessoais e operadores diferentes. Por outro lado, você não deve ser excessivamente granular ao inserir tipos de dados pessoais. Em vez de registrar todos os elementos de dados de um passaporte, não seria melhor dizer, "Detalhes do passaporte"?

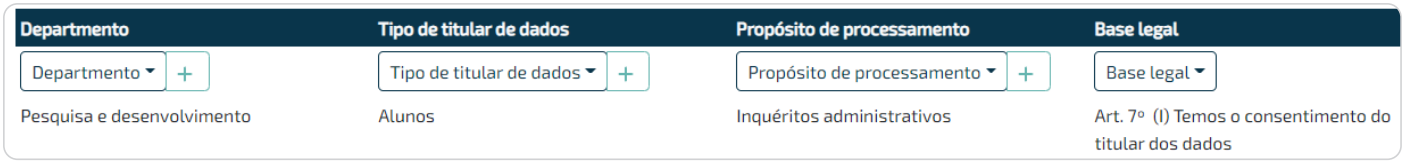
A granularidade também é importante quando se trata de Ativos de informação, (locais de processamento interno). Você não deve usar o termo 'Servidor de aplicativos', uma vez que pode não fazer sentido para alguém que gerencia solicitações de acesso dos titulares dos dados (DSR). Utilize um termo mais descritivo, que permita que a pessoa pesquise os sistemas ou aplicativos relevantes, ao procurar dados pessoais para responder a uma solicitação de acesso

O mapeamento de dados é feito em fases:

Em nosso exemplo, estamos fazendo **mapeamento de dados por departamento.**

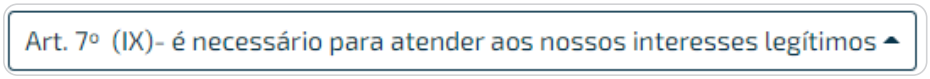
Descreva Quem?" (quem são os titulares) e "Porquê?" (propósito do tratamento de dados)

Para começar, selecione o Departamento da lista de drop-down (ou adicione novos elementos clicando na cruz verde)."

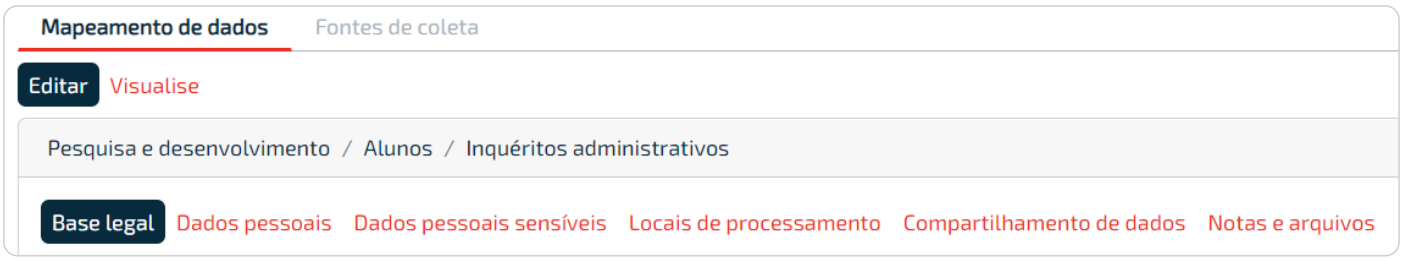


Selecione o departamento, o tipo de assunto de dados, a finalidade de processamento e a base legal. Em seguida, clicar em 'Adicionar novo' vai levá-lo para o próximo passo onde você descreve.

NOTA: Se você selecionar a base legal **Legitimo interesse**



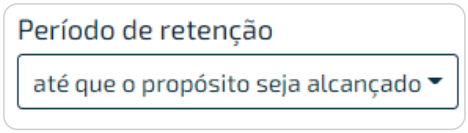
Na próxima seção você deve indicar o tipo de interesse legítimo e, você deve usar o modelo para concluir uma Avaliação de Legitimo Interesse (LIA ou Teste de Ponderação). Isso é feito para garantir que os interesses da sua organização não superem as expectativas dos titulares dos dados pessoais.



Clicar em 'Adicionar novo' abrirá a caixa acima onde você precisará:

Para este exemplo 'propósito', Inquéritos administrativos.

Digite **QUANTO TEMPO** (Período de retenção)? (você pode adicionar o seu próprio período, selecionando 'Outros')



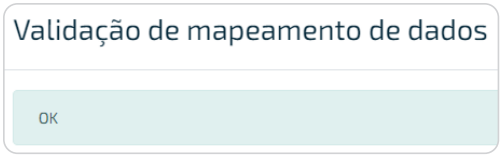
Digite os tipos de Dados Pessoais Descreva "Quais?" (Quais são os tipos de dados)

Digite os tipos de Dados Pessoais da Categoria Especial (Dados Sensíveis), incluindo uma **segunda base legal**.

Digite os locais de processamento, "Onde?" (Onde ficam armazenados). Internamente (dentro da organização) e/ou, externamente por qualquer operador.

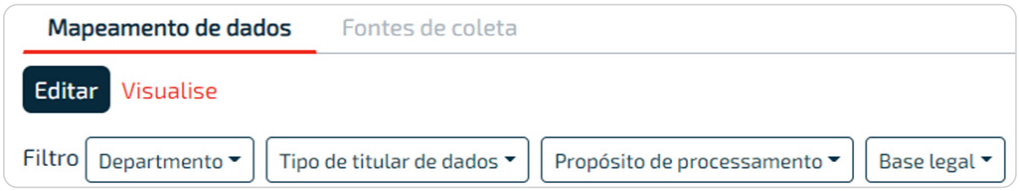
Em Compartilhamento de Dados, adicione todos os operadores com quem você divulga dados pessoais. Adicionar notas e arquivos relevantes.

Uma vez concluído, clique em 'Validar'. Caso não esteja completo, você será informado sobre onde completar seu mapeamento de dados.



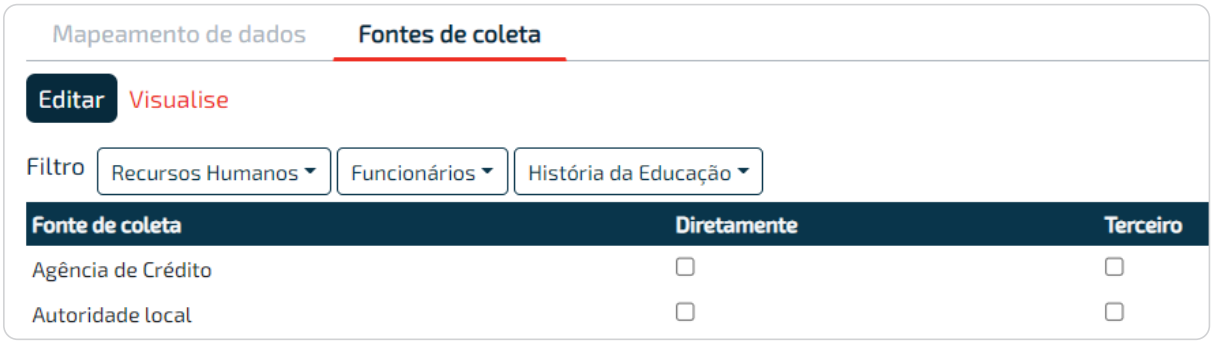
Continue o mapeamento de dados para o próximo novo conjunto de tipos de sujeitos de dados, propósitos. Use o Filtro se estiver editando as entradas existentes.

Continue o mapeamento de dados para o próximo novo conjunto de tipos de sujeitos de dados, propósitos. Use o Filtro se estiver editando as entradas existentes.



OU, vá para a Fonte de Coletas

Identifique a fonte de coleta



Depois de validar com sucesso cada seção do Data Mapping, indique a(s) fonte(s) de coleta para cada um dos dados pessoais ou tipos de categoria especial selecionados no mapeamento de dados.

Use o Filtro para selecionar o departamento, o tipo de assunto de dados e o tipo de dados pessoais. Selecione a fonte/s da coleção e se for de terceiros, digite a categoria de terceiros, por exemplo, Bureau de Crédito.

Clique em Validar. Se houver problemas, a validação informará sobre onde estão os problemas. Se você ver 'OK', passe para o próximo conjunto de fontes de coleta.

Obs. O mapeamento de dados se integrará ao **Relatório de Registros de Processamento (ROPA)** do módulo de Governança.

DICA: Em Fontes de Mapeamento e Coleta de Dados, clique em 'Visualizar' para obter uma visão geral do seu progresso.

Governança

A manutenção das configurações da organização e o mapeamento de dados, fornecem informações essenciais para os modelos de avisos de privacidade. No módulo Governança, o Registro atividades de Processamento (ROPA) deve ser mantido, Além dos documentos (politicas, avisos etc.) que você deve compartilhar com os funcionários.

Avisos de Privacidade

O LGPD tem requisitos específicos para notificar os Titulares sobre o tratamento dos seus dados, antes da coleta. A palavra-chave é - COLETA. Seu aviso deve ser exibido no ponto da coleta ou próximo.

Observe: Você poderá editar o Aviso de privacidade (externo) e a Política de Privacidade dos funcionários.

Há 3 opções.

1. O modelo que é atualizado a partir de configurações da organização e mapeamento de dados;
2. a versão editável onde você cria seu próprio conteúdo;
3. ou a opção de carregar seu próprio PDF.

Independentemente da opção, você deve se lembrar de atualizar **regularmente** o aviso de privacidade.

Uma vez publicado, defina o status como Concluído – isso atualizará seu painel de controle.

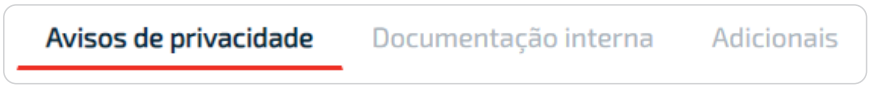
DICA: Lembre-se de publicar o aviso de privacidade dos funcionários também.

Integração com o WEBSITE

A opção de integração está ao lado da guia aviso de privacidade. Aqui você encontrará o **código que você pode incorporar em seus sites**. Quando as pessoas clicarem no seu link de aviso de privacidade, eles verão o que você publicou aqui. Há também a opção de baixar sua versão publicada, caso você compartilhe o aviso de privacidade por outros meios além dos seus sites.

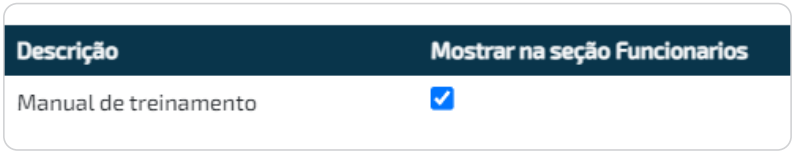
Não é recomendável que você apresente a Política de Privacidade em seus sites, mas você deve publicar e compartilhar internamente com os seus funcionários.

Treinamento e Conscientização



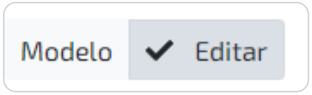
Uma das maneiras de demonstrar conformidade é mostrar como você promoveu o treinamento e a conscientização relevantes dentro de sua organização. Nestas guias você pode encontrar documentos para compartilhar com vários funcionários. Alguns deles têm as opções 'modelo', 'versão própria', 'upload'. Se você não quiser compartilhá-los, marque-os como N/A.

Na Biblioteca de Documentos você pode editar ou carregar seus próprios documentos. Se você quiser compartilhá-los, você deve marcar a opção 'Compartilhar com os funcionários'.



Medidas de Segurança

Para manter seu relatório registros de atividades de processamento, forneça uma descrição geral das medidas adotadas por sua organização que garantam um nível de segurança adequado aos riscos do processamento de dados pessoais. Quando sua organização processa dados pessoais em nome de outras organizações (o que faz de você um operador), forneça uma descrição geral das medidas de segurança organizacional que podem estar relacionadas especificamente a essas categorias de atividades de processamento

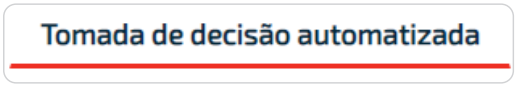


Registros de Atividades de Processamento

Para demonstrar o cumprimento do LGPD, o controlador ou operador deve manter os registros de atividades de processamento sob sua responsabilidade. Cada controlador e operador devem ser obrigados a cooperar com a Autoridade Reguladora (ANPD) e disponibilizar esses registros

Este relatório é atualizado automaticamente a partir da conclusão do mapeamento de dados e as medidas de segurança descritas acima.

Tomada de decisão automatizada



Se o perfil da sua organização, envolve processamento automatizado de Dados Pessoais para avaliar certos comportamentos relacionados a uma pessoa física; e se o processamento automatizado implicar na exclusão de qualquer intervenção humana na tomada de decisões sobre o perfil do titular. Neste caso você deve informar aos titulares dos dados os seus direitos associados, bem como as salvaguardas adequadas para garantir a segurança das informações.

Nota: O conteúdo capturado aqui atualizará o Aviso de Privacidade utilizado.

Conscientização de Funcionários

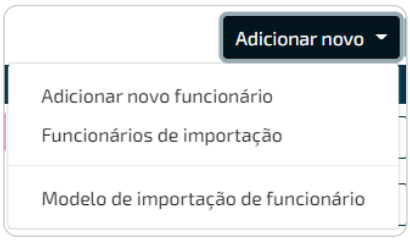
Todos os funcionários deverão estar diretamente envolvidos na implantação da Governança de privacidade e proteção de dados: gerentes, funcionários, diretores, administradores etc.

Uma das formas de demonstrar o cumprimento do LGPD, é mantendo todos os funcionários informados de suas funções, responsabilidades e políticas relacionadas à proteção da privacidade

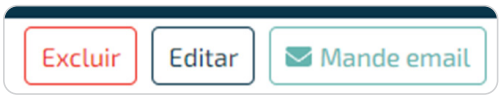
No módulo Governança você deve selecionar os documentos relevantes que deseja compartilhar com seus funcionários e contratados terceirizados.

Primeiro nome	Último nome	Cargo	Endereço de e-mail
AnaRita	Neves	CEO	dpo@lgpdconsulting.com

Você pode adicionar um funcionário individualmente ou usar o modelo (planilha .xls) para carregar um lote, e enviar para todos, clicando em 'Enviar e-mails'.

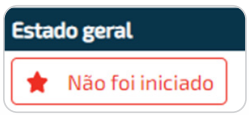


Nota: É possível enviar e-mail individualmente clicando em 'Enviar e-mail', ao lado do nome do funcionário. Você também pode personalizar suas mensagens.



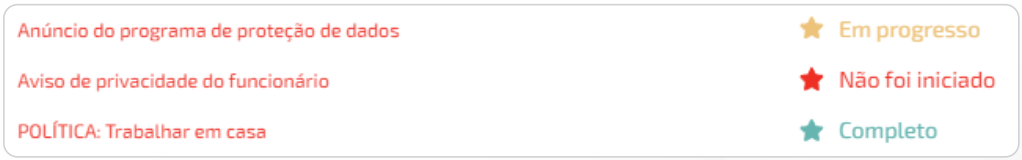
Os funcionários deverão abrir o documento "clicando no link no e-mail" , ler o documento e, em seguida, indicar a ciência do documento.

Nota: O status geral aparece ao lado de cada nome de funcionário.



Ao clicar em um funcionário, você verá o status de cada documento.

- **Uma estrela vermelha:** significa que o documento não foi enviado.
- **Uman estrela laranja:** significa que foi enviada, mas não há resposta.
- **Uma estrela verde:** significa que o empregado aceitou o documento.

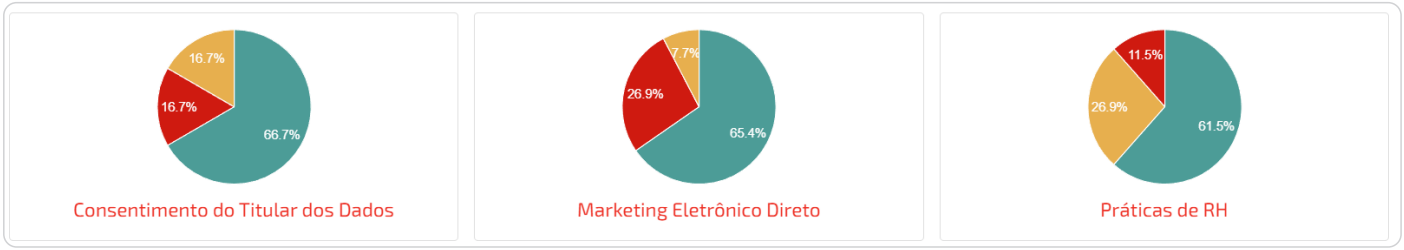


Conformidade e riscos

Operações envolvendo o processamento de dados pessoais exigem revisão, avaliação e manutenção regulares. Dependendo da estrutura da sua organização, você pode precisar envolver outros Proprietários de Informações, por exemplo: seu Gerente de RH, Gerente de TI, Gerente de Vendas etc.

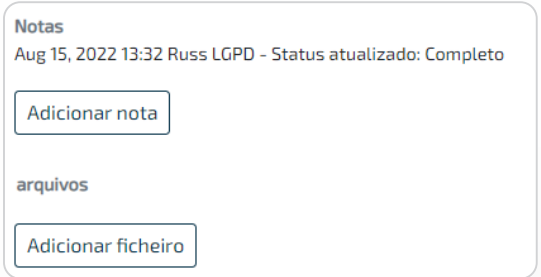
Quando você concluir o mapeamento de dados, você certamente descobrirá riscos operacionais e problemas (GAPS) que precisam ser gerenciados. Estes GAPS devem estar cobertos pelas seções de conformidade e tarefas padrão,

Nota: você poderá adicionar suas próprias seções e tarefas (questionários de avaliação personalizados).



A título de exemplo, vamos analisar 'Controles de Segurança' da seção 'Uso de Informações & Segurança'.

1. Você deve atribuir todas as tarefas da seção de conformidade aos Usuários de Conformidade. Adicione os usuários "clicando na cruz verde". Um usuário de conformidade só verão as tarefas a ele atribuídas.
2. Encontre informações úteis nas guias Rankings de Risco e fundamentação.
3. Adicione seus próprios questionários de avaliação na lista de verificação ou faça upload usando uma planilha (csv).
4. Atribua itens da lista de verificação aos Proprietários de Tarefas e, **o mais importante, defina um ciclo de revisão** que aciona notificações (lembretes) aos proprietários das tarefas.
5. Avalie o progresso da sua organização em cada item da lista de verificação: (Não começou; Em andamento; N/A; Completo)
6. Reinicie o nível de risco residual depois de definir seu Status (em **5.**)



NOTA: Clicando na seta de esquerda à direita, o proprietário da tarefa pode adicionar notas de auditoria e carregar documentos em apoio à revisão.

A definição de itens para completar no Uso de Informações & Segurança também atualizará o **Relatório** de **Registros de Atividades de Processamento (ROPA) do módulo de** Governança.

GRANDE DICA: Ao clicar na cruz branca no círculo verde, você pode adicionar suas próprias seções e itens de lista de verificação em cada seção. Este recurso é especialmente útil quando você precisa gerenciar riscos e problemas que você identifica durante o procedimento de avaliação de Governança Organizacional ou durante operações corriqueiras.

Relatório de avaliação

Execute este relatório para acompanhar e informar sobre sua jornada de conformidade. Use filtros para atingir seções específicas. Baixe o relatório em formato PDF ou Excel.

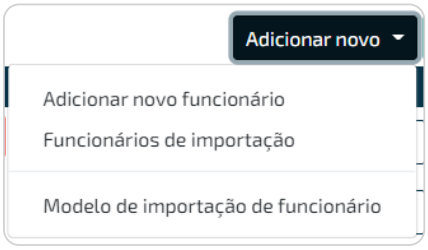
É uma boa prática executar regularmente e imprimir o relatório completo.

Operadores

Um operador é uma pessoa/organização que processa dados pessoais em seu nome (controlador), sob um contrato vinculante. Eles não podem usar os dados pessoais para seus próprios propósitos. Um exemplo seria uma empresa que faz processamento de folha de pagamento em nome da sua empresa.

Note que há uma lista de verificação (Due Diligence) do operador. Quando você adiciona qualquer Operador no mapeamento de dados, eles aparecem nesta seção.

Neste módulo são mantidos os contratos firmados com os Operadores. Você pode adicionar um modelo personalizado ou usar o modelo de padrão.



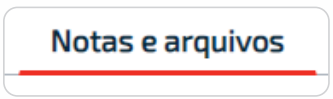
A LGPD não informa quem deve elaborar o contrato bilateral, mas exige que o Controlador (sua organização) deve garantir que o contrato escrito defina medidas de segurança adequadas, que o Operador deve implementar e manter.

Edite o formulário **(1)** completando os detalhes do contato, a data de início e término do contrato.

Defina o status e salve o formulário. O status será exibido aqui **(2)**, uma vez que você tenha o contrato assinado, carregue-o aqui **(4)**

Quando você estiver transferindo dados pessoais para fora do Brasil, certifique-se de indicar a base legal adequada. **(3)**

Novo recurso – Agora você pode adicionar Notas e Arquivos para cada Operador.



Compartilhamento de Dados

Ao contrário do 'compartilhamento' de dados pessoais entre Controlador e Operador (que está sob contrato escrito), aqui tratamos do compartilhamento ou divulgação de dados pessoais *entre controladores*.

Um exemplo pode ser quando uma organização fornece seguro médico aos seus funcionários. Neste caso, deve existir um tipo de acordo formal reconhecido entre as duas organizações.

Basta carregar uma cópia do acordo vinculante e definir o status como Assinado.

As funcionalidades dentro deste módulo são idênticas à seção Operadores, exceto que os links externos são relevantes para as relações controlador-controlador.

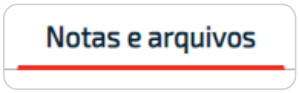
Vejamos um outro exemplo simples:

Digamos que um agente de viagens faça reservas, em nome de seus clientes, com uma companhia aérea e uma rede de hotéis. Neste caso a rede de hotéis e a companhia aérea não podem ser considerados Operadores e sim Controladores.

Entretanto, se as três empresas se reunirem para desenvolver um sistema ou aplicativo que agregue valor para todos os seus clientes, neste caso estamos falando de *um processamento adicional* que caracteriza uma relação **de compartilhamento conjunto** – e exigirá definitivamente o consentimento dos titulares dos dados. Na verdade, todas as outras hipóteses legais devem ser consideradas.

É importante que o titular dos dados saiba a quem abordar.

Novo recurso – quando você editar um Controlador, agora você pode adicionar Notas e Arquivos

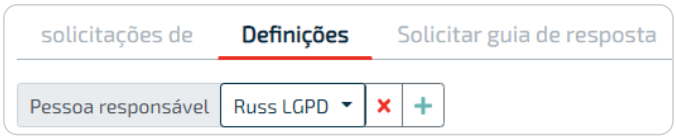


Requisição de acesso aos dados do titular

Existem várias razões pelas quais os Titulares podem querer ter acesso aos seus dados pessoais e exercer seus direitos e garantias sobre eles. Existem várias maneiras pelas quais os titulares dos dados podem fazer essas solicitações de acesso. Da mesma forma, existem várias respostas diferentes que podem vir de sua organização.

O PrivIQ fornece aos solicitantes um link on-line, e permite que você receba ou capture as solicitações, para que possa delegá-las com eficácia. A plataforma permite navegar, entender as regras e acompanhar o progresso das demandas, através de um painel de controle.

Configurações

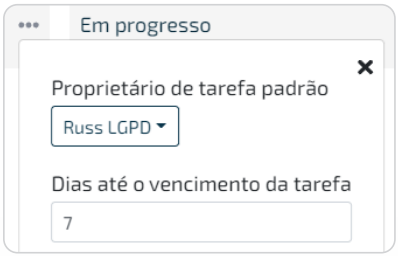


Clique em Configurações e defina o 'Responsável' para receber solicitações online.

Se não estiver no drop-down, clique na cruz verde para adicionar novas pessoas.

O 'Responsável' deve definir a **Preferência de Notificação**, para ser alertado quando uma solicitação de acesso on-line for recebida. Para fazer isso, clique no nome de usuário no canto superior direito.

As seções 'Recebidas' e 'Em progresso' têm 3 pontos. Defina o proprietário da tarefa padrão e o número de dias dentro dos quais ele deve responder.



Integração do formulário de solicitação de acesso on-line (DSAR)

Em Configurações – peça ao seu desenvolvedor web para incorporar o código por trás de um link em seu site.

Nomeie como "Requisições de acesso aos dados do titular (**DSAR**) '.

Adicione os domínios que disponibilizarão este link.

Clique em 'Visualizar' para ver como ele se apresentará ao solicitante.

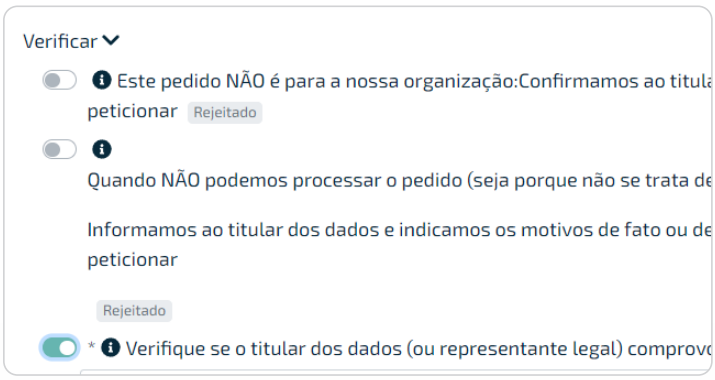
Solicitações

As solicitações online são recebidas automaticamente aqui. Você pode adicionar solicitações manualmente clicando em Adicionar novo

Olhando para o painel acima, podemos ver o número de referência automaticamente atribuído **(1)**, a data de vencimento **(2)** e o botão de download, **(3)**

Clique em um painel para entrar. Ao clicar em Progresso, você notará as 3 estágios – **Recebido, Em Andamento e Completo**.

Recebido



Avalie a solicitação DSAR, pois pode haver razões legais pelas quais você pode rejeitá-la.

Se for um pedido legítimo, indique como você provou a identidade do solicitante.

Clique no botão Mover para habilitar o Progresso.

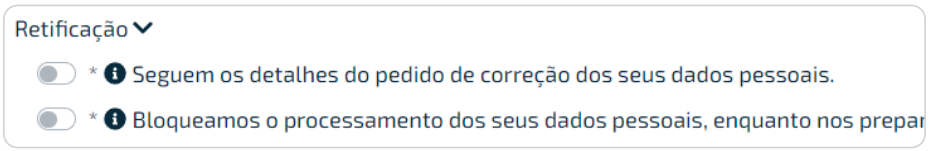
Em andamento

Se o mapeamento de dados for preciso e atualizado, ele deve lhe dar uma indicação clara de onde pesquisar os dados.

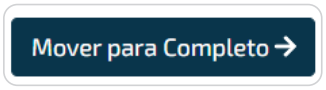
Caso você considere qualquer um dos mapeamentos incompletos, informe ao seu gerente de privacidade para atualizá-lo.

Uma vez que você tenha localizado todos os dados para apoiar sua decisão, passe pelas regras.

A regra com uma estrela **é obrigatória**. Passe o mouse sobre o texto para ver informações de suporte. O texto azul indica que a solicitação foi bem-sucedida e o texto vermelho significa que falhou.



Se você tiver seguido as etapas corretamente, você poderá mover a solicitação para a coluna Completa.



Gerenciamento de violações

Uma violação de dados pessoais ou incidente de segurança, pode levar ao uso acidental ou ilegal, destruição, perda, alteração ou divulgação não autorizada dessas informações.

Uma violação, não corrigida adequadamente, pode resultar em estresse físico, material ou moral aos titulares dos dados e pode também causar um impacto negativo financeiro e/ou na reputação da sua organização.

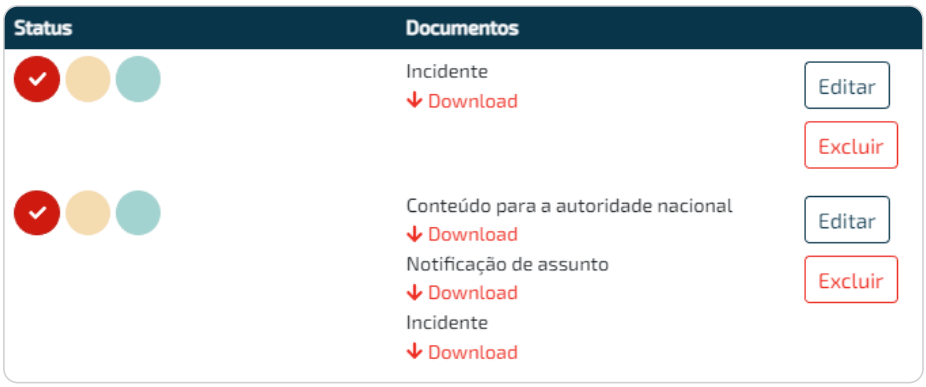
Um Controlador deve informar a Autoridade/ Reguladora, o mais rapidamente possível, um incidente de segurança que possar causar dados graves e irreversíveis aos titulares.

O Controlador também precisa comunicar aos titulares dos dados, especialmente quando a exposição apresenta um alto risco para eles.

O Controlador deve considerar a possibilidade de alertar as autoridades policiais, que possam estar envolvidas. Por exemplo, quando envolve questões de segurança ou quando a divulgação antecipada dos Titulares dos dados pode dificultar as investigações.

Use esta seção para gerenciar suas respostas a incidentes, bem como para notificar a Autoridade / Reguladora e aos Titulares de dados. Certifique-se de que seu operador tenha um processo semelhante.

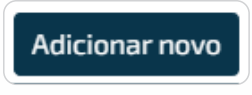
OBS. Fazer treinamentos de conscientização de segurança com a equipe, promove boas práticas e mantém a os funcionários cientes dos processos envolvidos na gestão de resposta a falhas. Imprima os certificados como evidência de treinamento.



No exemplo acima temos dois tipos de incidentes:

1. O primeiro em que o incidente foi contido sem graves prejuízos. Nesse caso não há necessidade de comunicar a Autoridade/ Reguladora, nem aos Titulares dos dados, mas há necessidade de elaborar um relatório do incidente.
2. Um Incidente Grave deve ser comunicado tanto à Autoridade/ Reguladora, quanto aos sujeitos de dados impactados.
   OBS. em alguns casos, você pode ser impedido legalmente de informar o incidente aos Titulares dos dados.

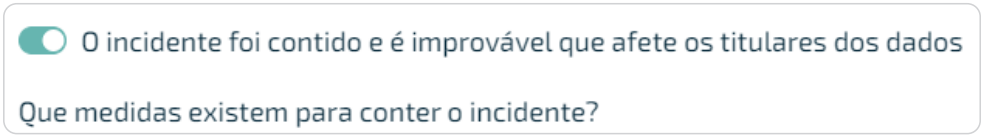
Clique em Adicionar novo



Leia a Introdução na seção **Contenção & Recuperação.**

Preencha o título e os detalhes do Incidente.

Em seguida, estamos na etapa de **Avaliação de Risco.**



Vá para a etapa final que é a **avaliação e resposta do incidente**.

Ao Clicar em 'Terminar' um Relatório padrão de Incidentes é produzido.

No entanto, se o incidente *não* tiver sido contido, você deverá passar pelas etapas até enviar notificação à Autoridade /Reguladora.

Obs. Aqui você encontrará todo o conteúdo para elaborar o relatório para a Autoridade Reguladora.

Na página seguinte encontra-se o conteúdo para enviar a comunicação aos titulares dos dados, afetados pelo incidente.

NOTA: Aplicação da lei – Se você tiver selecionado este item na sua Avaliação **de Risco**, o conteúdo que normalmente seria usado para comunicar os Titulares de dados não será exibido.

Avaliação de impacto de proteção de dados (DPIA)

A condução de um DPIA ou RIPD-Relatório de Impacto de Proteção de Dados é um requisito legal obrigatório, para ajudar a atender às expectativas de privacidade e proteção de dados de clientes, funcionários e outras partes interessadas. Este documento demonstra os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados

A elaboração do DPIA é uma prática prospectiva e proativa, que funciona como um sistema de alerta antecipado, considerando os riscos de privacidade e conformidade no projeto inicial e em todo o projeto (Privacy by Design).

Esta seção permite identificar se o DPIA é relevante para seu projeto.

A DPIA é um documento projetado para descrever o processamento, avaliar sua necessidade e proporcionalidade e ajudar a gerenciar os riscos aos indivíduos, resultantes do processamento de dados pessoais. Ele serve como evidência em uma possível em investigação, pois pode ajudar o Controlador a demonstrar que medidas de segurança apropriadas foram adotadas, para garantir o cumprimento à LGPD.

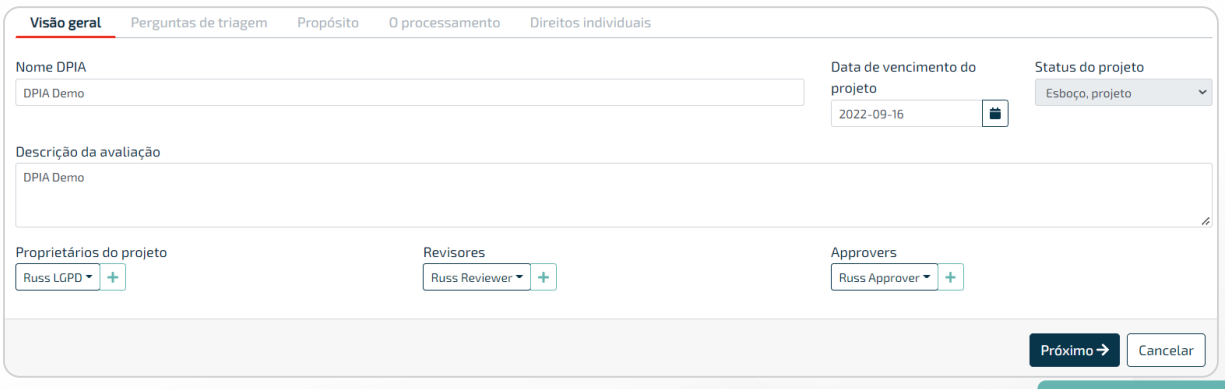
Alguns exemplos de onde uma DPIA pode ser necessária:

- Um hospital processando os dados genéticos e de saúde de seus pacientes;
- O uso de um sistema de câmeras para monitorar o comportamento da condução nas rodovias. O controlador de dados prevê usar um sistema inteligente de análise de vídeo para destacar carros e reconhecer automaticamente placas de carro;
- Uma empresa que monitora as atividades de seus colaboradores, incluindo o monitoramento da estação de trabalho dos funcionários, atividade na internet etc.
- A coleta de dados públicos de perfis de redes sociais, por empresas privadas gerando perfis para diretórios de contatos

Nota. Em alguns casos o processamento pode exigir consulta prévia da Autoridade Reguladora

Clique:

Digite o Título do DPIA e detalhes: data de vencimento, Descrição e Progresso. Clique em **Salvar**



O **proprietário do Projeto** geralmente é a pessoa que compila e edita o DPIA.

Selecione o (s) Revisor ou adicione qualquer um que não esteja na (clique na cruz verde).

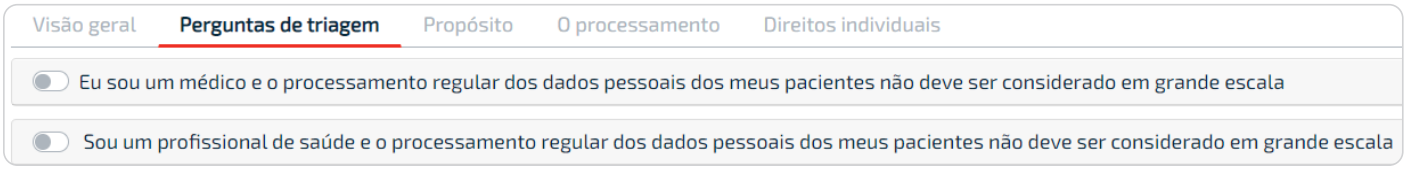
Os revisores só podem ser Usuários de Conformidade ou Proprietários de Tarefas.

Selecione o **Aprovador**(s), ques devem ser usuários do tipo Administrador.

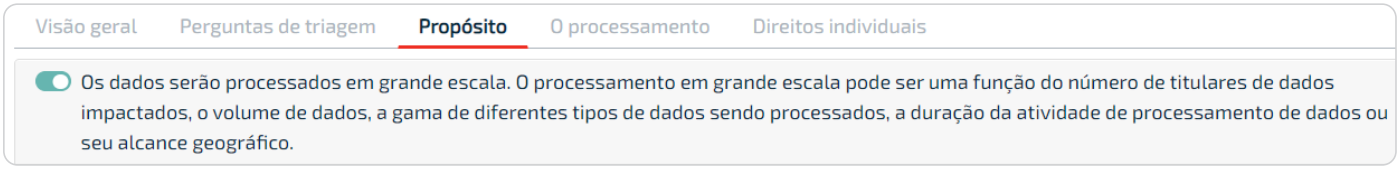
Os comentários e orientações do DPO no DPIA serão gravados como tal. Indique se o usuário é o DPO da Organização.

Perguntas de Triagem

Ao selecionar as opções em perguntas de triagem, você determina se um DPIA é ou não relevante ou necessário.



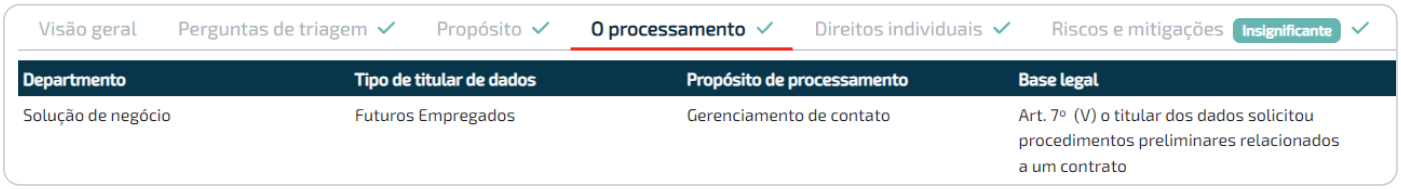
Propósito



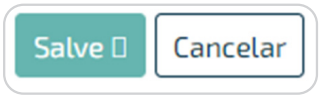
Nesta seção, você indica *porquê* o DPIA é relevante para este projeto ou processamento planejado de dados pessoais.

Você pode editar ou carregar documentos, clicando em 'Notas e Arquivos', para justificar sua própria razão para conduzir um DPIA.

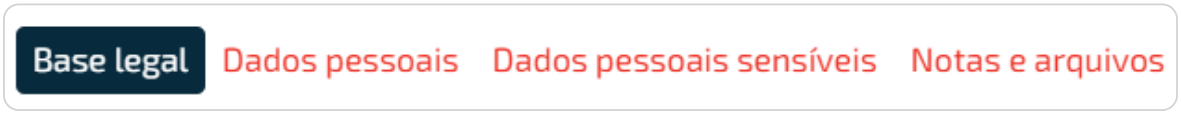
Justificativa de processamento



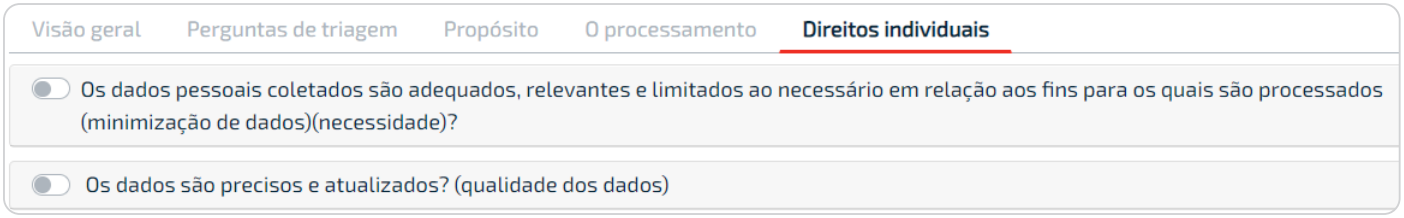
Selecione o departamento / tipo de assunto de dados / propósito de processamento e base legal. Em seguida, clique em **Salvar**.



No painel seguinte, complete os campos obrigatórios (destacados em vermelho), com os tipos de dados pessoais relevantes, se necessário, adicione notas e arquivos e, em seguida clique em Fechar.



Direitos individuais

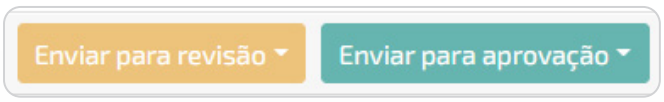


Esta seção diz respeito aos direitos dos Titulares dos dados e **como esses direitos serão protegidos**. Depois de concluir esta seção, o DPIA estará pronto para ser enviado para a **primeira revisão.**

Depois de revisado o DPIA deve ser encaminhado para aprovação.

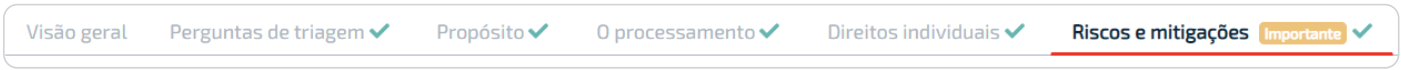
O **revisor** e o **aprovador** receberão notificações informando-os sobre as suas respectivas tarefas.

Após inserir seus comentários, o revisor pode retornar o DPIA para melhoria ou encaminhá-lo para o **aprovador**.



Riscos e Mitigações

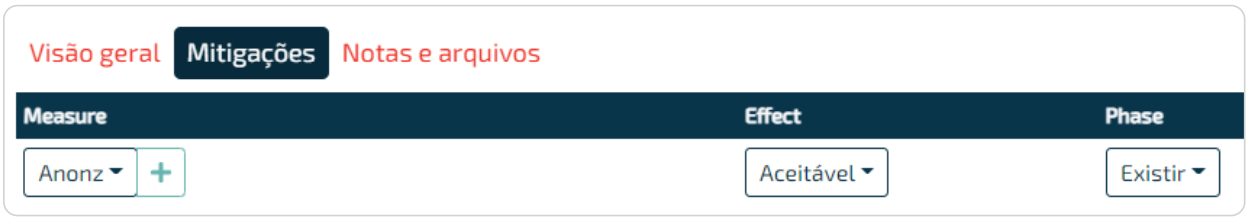
Nesta seção o proprietário do DPIA deve avaliar os riscos e as salvaguardas utilizadas para mitigar os riscos de incidentes de segurança.



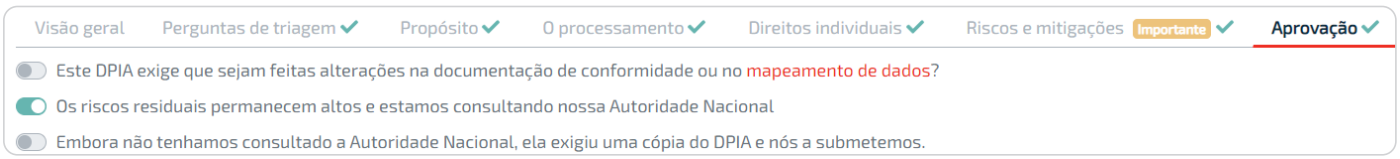
O proprietário do DPIA deve adicionar um risco relevante e clicar em Salvar.

Em seguida, deve adicionar o respectivo controle de segurança para mitigar o risco.

NOTA: Uma vez adicionado um controle de segurança, ele não poderá ser editado, você deve exclui-lo e em seguida substituir pelo correto.

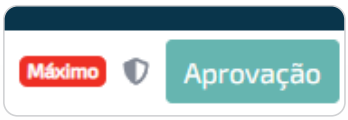


Quando todos os riscos e mitigações forem assinalados, envie o DPIA para aprovação.



Aprovação Final

Aprove cada risco individualmente, clicando em **Aprovação**. Clique em Fechar e retorne à página principal de aprovação.



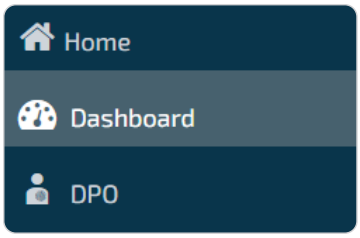
Em seguida, aprove os riscos em geral adicionando comentários, clique em Aprovação, na parte inferior da página, e encaminhe para o proprietário.

Há dois resultados possíveis após a aprovação final:

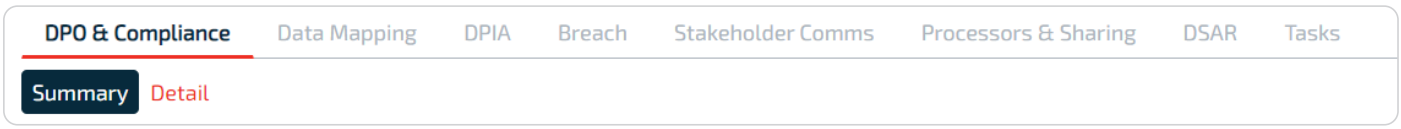
- O proprietário pode utilizar informações do DPIA para completar o módulo de gerenciamento de riscos de seus projetos.
- Caso seja necessário, o DPIA deverá ser submetido para avaliação da Autoridade Reguladora.

Painel de Controle

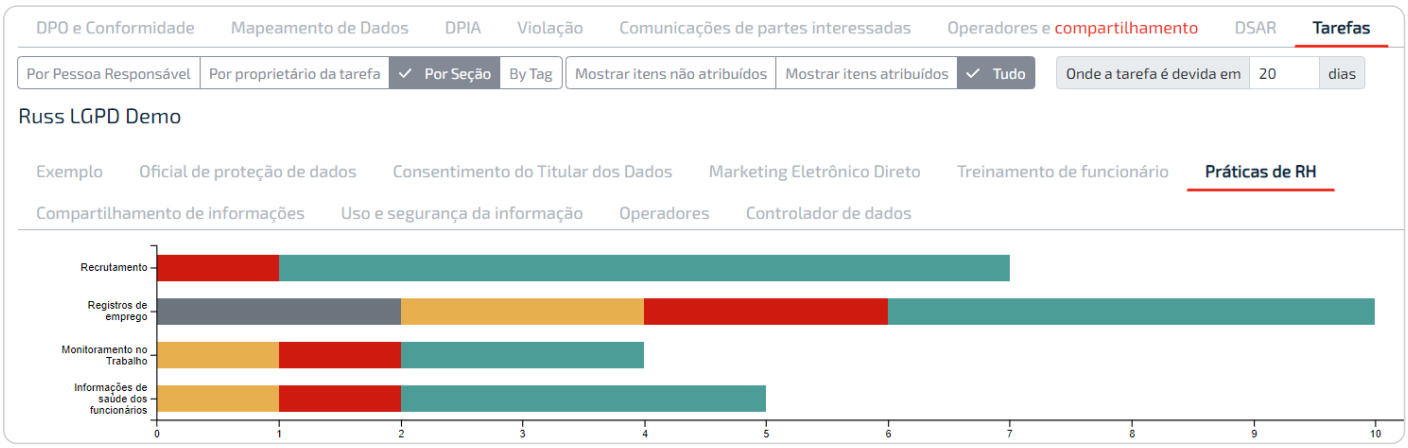
Encontre o ícone do painel na barra lateral.



Você pode ver através das várias seções.



Você e gerar visões ou relatórios a partir da combinação de vários critérios, por exemplo: pesquisar todas as tarefas de determinado proprietário.



Manutenção do usuário

Adicione e gerencie usuários do sistema.

Aqui você deve adicionar usuários de conformidade, para possibilitar que eles tenham sido designados como o responsável nas seções de Conformidade.

Autenticação Multifator -MFA

Para fornecer uma camada extra de segurança, você deve configurar a autenticação multifatorial (MFA).

Novos usuários receberão um e-mail de boas-vindas, convidando-os a fazer login com uma senha temporária e, em seguida, alterando sua senha.

Você pode optar por receber um código de verificação via SMS, que você irá inserir junto com a senha.

Você também pode usar um autenticador, como Authy, Google Authenticator (iOS/Android) ou Microsoft Authenticator, que irá gerar o código de verificação para entrar com sua senha.

Glossário

Titular dos Dados –Pessoa física a quem os dados pessoais objeto de processamento se referem

Dados Pessoais – significa qualquer informação relacionada a uma pessoa natural identificada ou identificável

Controlador – pessoa física ou jurídica, de direito público ou privado, que tenha competência para tomar as decisões relativas ao tratamento de dados pessoais

Operador – pessoa física ou jurídica, de direito público ou privado, que processa dados pessoais em nome do responsável pelo tratamento (controlador)

Titular da Informação - um indivíduo que aprovou a responsabilidade gerencial pelo controle da manutenção, uso e segurança dos seus dados pessoais

LGPD – Lei de Proteção de Dados Pessoais

DPIA – Avaliação do Impacto de Privacidade equivalente ao RIPD (Relatório de Impacto de Proteção de Dados) na LGPD

MFA – Autenticação multifatorial

Implementation Guide

This guide may be used where your country's regulation and terminology are like that of the LGPD. Sections like the DPO are specific to the LGPD and may not apply to your regulation.

Your organisation is the **Controller**. We suggest you adopt the following approach to rolling out your privacy compliance program.

1. Understand the organisation's activity by asking:
    - what are the core activities?
    - how many employees?
    - do you outsource the processing of personal data?
    - do you disclose personal data to other organisations?
    - do you transfer personal data outside your country or region?
    - who heads up departments, e.g., HR, Sales and others that deal with personal data?
    - who is leading the privacy program?

2. Heads of departments (**Information Owners**) to formulate a list of ALL processing activities that involve personal data; including any informal activities. If possible, record the sources of the personal data, in which applications do they process personal data, where the information is stored in their departments, and to whom the information is disclosed. Include physical media as well.

3. Heads of IT / Procurement to compile a list of all Vendors involved with processing of personal data, the country in which they are located, the expiry date of those contracts.

4. Inform the CEO / MD / head of organisation of the data protection program.

5. Appoint the Data Protection Officer, where appropriate.

6. Register with the Relevant Authority, where required.

7. Ensure your Organisation Settings are complete. (See next section).

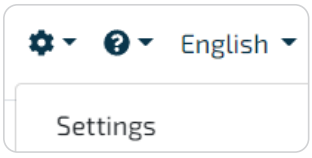
8. Add the relevant heads of departments and the program lead as users with the system role of Administrator. (Compliance User and Task Owner must be added via the Compliance sections).

9. Following point 2. above, Information Owners to review and understand ALL processing of personal data in their respective departments. Be aware of and record all *informal* processing too. For example, populating spreadsheets to manage processes outside of the formal, networked and security protected systems and apps.

10. Begin the data mapping exercise, using the prep work done by the Information Owners and record any work to be done beyond this session. The head of IT could provide valuable insight or guidance especially around any processing of personal data that may be outsourced to **Processors** as well as the processing done by IT. Set a date for a follow-up data mapping session. Use the follow-up session to complete the data mapping exercise.

Organisation Setup

To get to Settings, click the wheel in the upper navigation bar.



Under **'Your Organisation'** enter your contact details and upload your logo.

Under **'Your Location'** enter your physical and postal addresses. Ensure that you select the relevant supervisory authority. Ensure that a time zone is selected. (Only in GDPR).

Under **'Your Officers'** enter the organisation lead's (e.g., the CEO) name and email address as well as the DPO's details, where available.

Under **'Your Plan'** you will find the settings and features that determine your package size. Be aware of switching between data mapping by department. **Any data mapping done prior to your switching will be lost.**

Key Terms

These key terms are essential to the proper interpretation of LGPD and to maintain the app.

Data Controller – natural person or legal entity, of public or private law, that has competence to make the decisions regarding the processing of personal data.

Data Processor – natural person or legal entity, of public or private law, that processes personal data in the name of the controller.

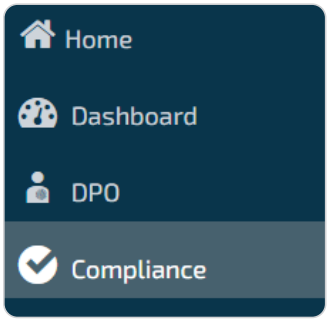
Personal Data – information regarding an identified or identifiable natural person.

Data Subject – means the person to whom personal data relates.

Information Owner – an individual that has approved management responsibility for controlling the maintenance, use and security of the personal data

Home Page

The features you see on the home page will be those that were selected under Your Plan in the Organisation Settings. When switching between different sections you are encouraged to use the sidebar.



At other times it might be convenient to click on the breadcrumb, as in the below picture where you're simply moving 1 level back to 'Information Use & Security'.

Data Mapping

Remember that saying regarding risk – "you can't manage it if you can't see it"? If people make enquiries about their personal data, or there's an incident, you need a detailed map to help you respond. But data mapping is much more than producing an inventory.

This represents the first step towards building a proper foundation upon which to manage your compliance program. The who, why, when, where and what of processing. Throughout the process you may add your own data items, should the default items not be sufficient.

Information owners must direct the data mapping and be involved throughout the process. Identify any informal processing and record it in the data mapping. These are typically the areas of vulnerability, and any risks or issues should be documented and managed in the relevant compliance section.

Before you begin, a word on granularity

Granularity is important when describing your processing purposes. Don't crowd many types of processing into a singular description, especially where there are different types of personal data, and different **Processors**. At the same time, you don't want to be overly granular when entering personal data types. Rather than recording every data element in a passport, would it not be better to say, "Passport details"?

Granularity is also important when it comes to Information Assets (in-house processing locations). You don't want to use 'Application Server' when that could be meaningless to someone who manages subject access requests. Add a location that is more descriptive, that enables the person to search the relevant systems or apps when searching for personal data to be used in response to a subject access request.

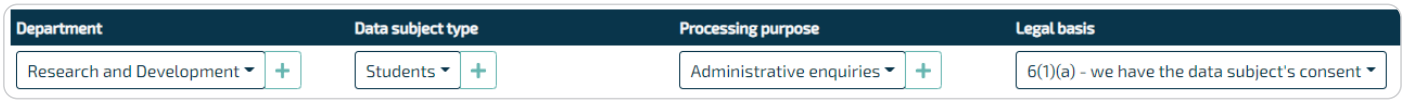
If there are commercial sensitivities around having the names of **Processors or Controllers** on your privacy notices then, add them as category names here and then add them individually in the Processors or Data Sharing sections, respectively. For example, you might not want to use 'Paula's Payroll Services', but rather use 'Payroll Processing Company' instead.

Data mapping is done in phases:

In our example, we're doing **data mapping by department.**

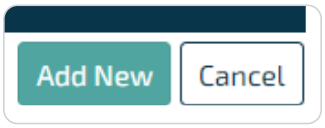
Record the 'who' and 'why'

To begin, select the relevant data elements from the drop-down lists (or add new elements by clicking the green cross).

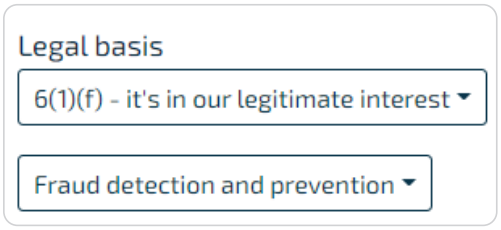


Select the department, data subject type (WHO), processing purpose (WHY) and lawful basis.

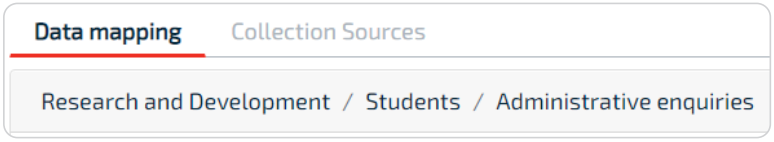
Then, clicking 'Add New' will take you to the next step where you describe the 'what' and 'where'.



NOTE: If you select the lawful basis – ***'it's in our organisation's legitimate interest',*** in the next section you must indicate the type of legitimate interest and, you should use the template to complete a legitimate interest impact assessment. This is done to ensure that your organisation's interests don't outweigh those of the data subject.



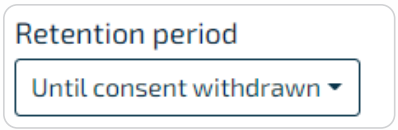
Describe the 'what' and 'where'



Clicking 'Add New' earlier will open the above box where you will need to:

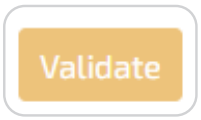
For this example 'purpose', …Administrative enquiries…

Enter the Retention Period (you may add your own by selecting 'Other')



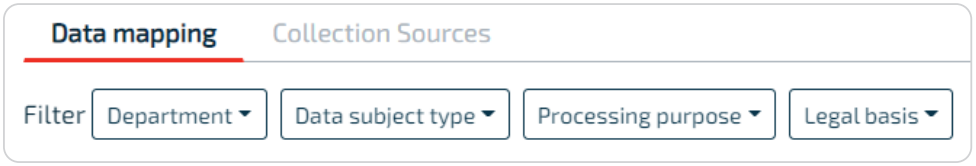
Enter the **Personal Data** types
Enter the **Special Category Personal Data** types, including that **second lawful basis**
Enter the **Processing locations**, In-house (within the organisation) and, externally by any **Processors** (See the earlier note on granularity)
Under **Data Sharing**, add any **Controllers** to whom you disclose personal data
Add relevant **Notes and Files**.

Once you're happy with your input, click 'Validate'



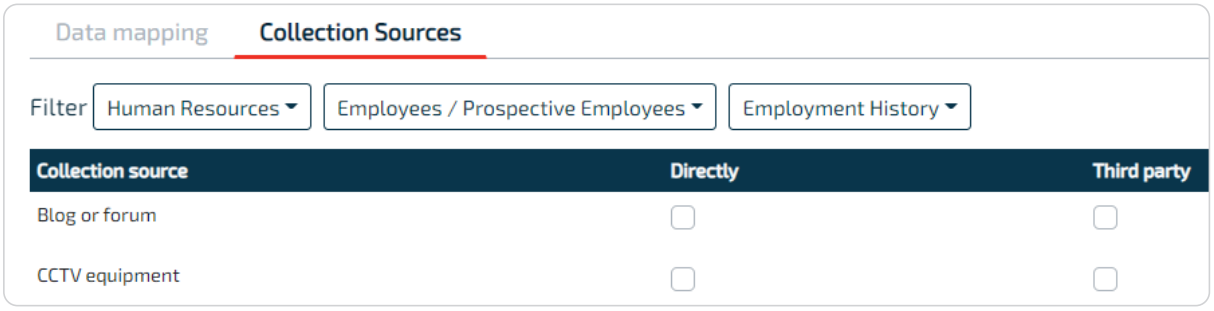
If you see 'OK', then you're done with this piece of data mapping. If not, you will be informed as to where to complete your data mapping.

Continue data mapping for the next new set of data subject types, purposes. Use the Filter if you are editing existing entries.



OR, go to Collection Sources.

Identify the collection source



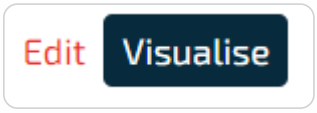
After successfully validating each section under Data Mapping, indicate the Collection Source/s for each of the personal data or special category types you selected in the data mapping.

Use the Filter to select the department, data subject type and personal data type. Select the collection source/s and if it's from a Third Party, enter the category of the third party e.g., Credit Bureau.

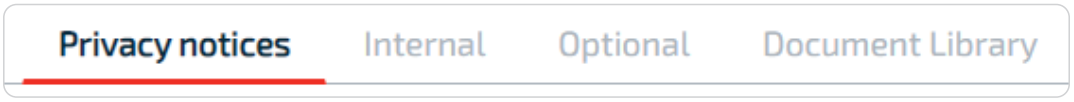
Click Validate. If there are issues, the validation will inform you as to where the issues are. If you see 'OK', move on to the next set of collection sources.

Data mapping will integrate with the **Records of Processing Report** which you will find under Governance.

HINT: In Data Mapping and Collection Sources, click 'Visualise' to get an overview of your progress.

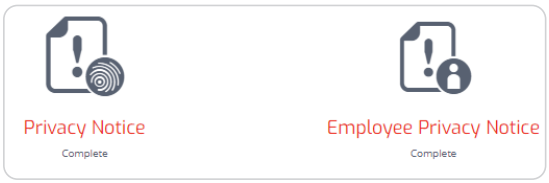


Governance

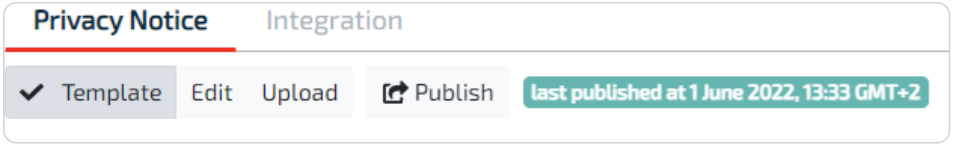


Maintenance of your organisation settings and your data mapping provides essential information to your privacy notices templates. In Governance, the Record of Processing must be maintained and there are documents that you need to share with employees.

Privacy Notices



The LGPD has specific requirements for notifying individuals when collecting their personal data. The keyword being – collecting. Your notice must be displayed at or near the point of collection. Notice the external Privacy Notice as well as one for Employees. Click 'Privacy Notice'.



There are 3 options. The template which is updated from organisation settings and data mapping; the editable version where you create your own content; or the option to upload your own PDF. Regardless of the option, you must remember to regularly **Publish** the privacy notice.

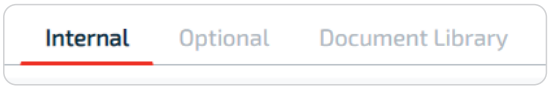
Once published, set the status to Completed – this will update your dashboard.

Remember to publish the employee privacy notice too.

Integration

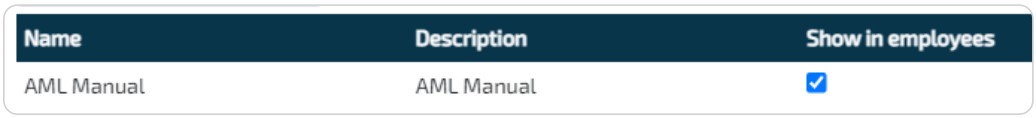
The integration tab is next to the privacy notice tab. Here you will find the **code that you can embed in your websites** so that when people click on your privacy notice link, they will see whatever you have published here. There is also the option to download your published version in case you share the privacy notice other than via your websites. It is unlikely that you will present your employee privacy notice on your websites, but you must publish it before you share with your employees.

Training & Awareness



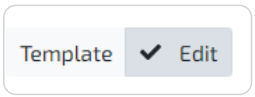
One of the ways to demonstrate compliance is to show how you have promoted the relevant training & awareness within your organisation. In these tabs you can find documents to share with various employees. Some of them have the 'template', 'own version', 'upload' options. If you are going to share a document with employees and other stakeholders, **you MUST set the document status to 'Complete'.** If you don't want to share them, mark them as N/A.

In the Document Library you can edit or upload your own documents. If you want to share them, you must tick 'Share with Employees?'



Security Measures

To maintain your Records of Processing Activities report, provide a general description of the measures adopted by your organisation which ensure a level of security that is appropriate to the risks of the processing of personal data. Where your organisation processes personal data on behalf of other organisations (and makes you a processor), provide a general description of the organisational security measures that might relate specifically to those categories of processing activities.



Records of Processing Activities

To demonstrate compliance with the GDPR, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the Authority / Regulator and make those records, on request, available to it, so that it might serve for monitoring those processing operations. This report is automatically updated from having completed your data mapping and the security measures outlined above.

Automated Decision Making

Profiling' involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Automated processing implies the exclusion of any human intervention in any decisions which may be taken about such profiling. This is where you inform data subjects of their associated rights as well as the suitable safeguards.
Content captured here will update the Template Privacy Notice.

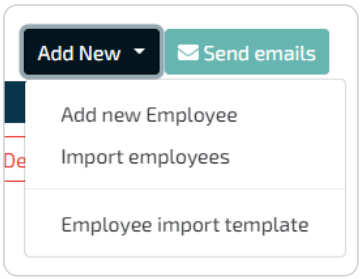
Employee Communications

Employees are directly involved in the organisation – managers, employees, directors, trustees etc. One of the ways in which to demonstrate compliance with LGPD is by keeping all employees informed of their roles and responsibilities towards privacy protection. In the Governance section you would have selected the relevant documents that you would need to share with your employees, contractor workers, and the like. Go to the Compliance section.

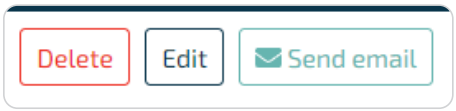
First name	Last name	Job title	Email address
Timmy	Thomas	None	timmyt@geemail.com

NOTE: You will only be able to select documents that have been set as 'Complete' in the Governance section.

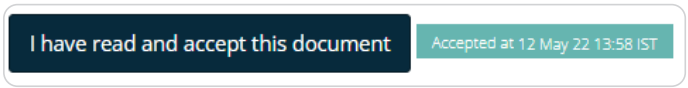
You may add an employee individually or use the template to upload. You may send emails globally, i.e., to everyone, by clicking 'Send emails'…



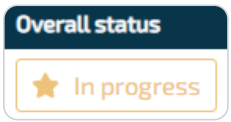
Or you can email individually by clicking 'Send email' next to the employee's name. You can also customise your message to the individuals.



They will need to open that document by clicking the link in the email, reading the document, and then clicking 'I have read and accept this document'.



The overall status appears next to each employee name.

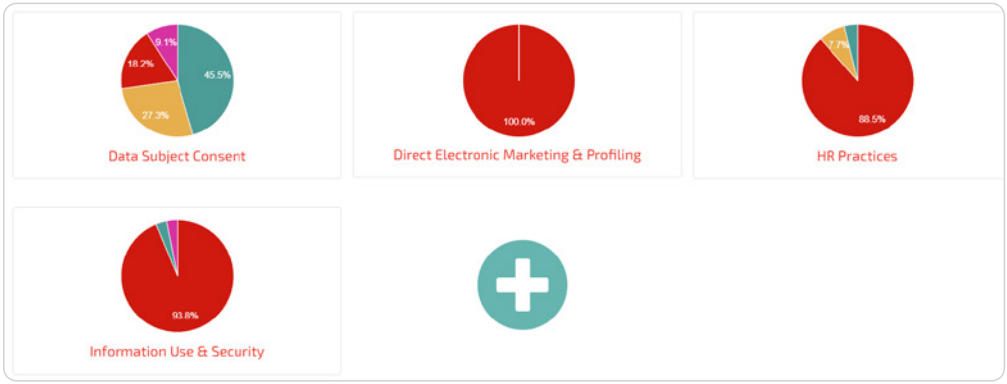


If you click on an employee, you will see the status of each document. A red star means the document has not been sent. An orange star means it has been sent but there is no response. A green star means the employee has accepted the document. Hover over the stars to see the meta-data.

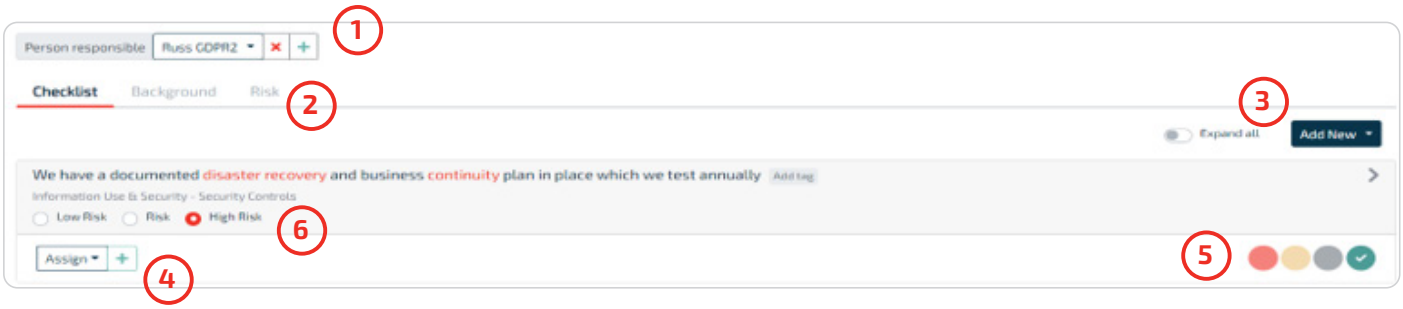
Document	Status
Data Protection Program Announcement	Complete
Employee Privacy Notice	Complete
POLICY: Working From Home	In progress
POLICY: Personal Data Breach	Not started

Compliance

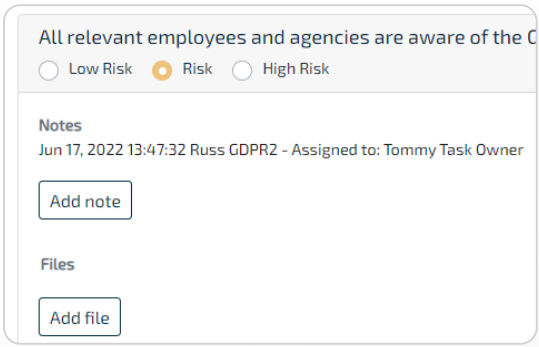
Operations involving the processing of personal data require regular review, assessment, and maintenance. Depending on your organisation's structure, you may need to get others involved – the Information Owners, e.g., your HR Manager, IT Manager, Sales Manager etc. When you do your data mapping you will almost certainly uncover operational risks and issues that need to be managed. If these are not covered by the default sections and tasks, you may add your own sections and tasks.



By way of example, let's look at 'Security Controls' which you will find under 'Information Use & Security'.



1. You MUST assign all compliance sections to Compliance Users. If not in the drop-down list, add users by clicking the green cross. A compliance user only sees sections assigned.
2. Find useful information in the Background and Risk Rankings tabs.
3. Add your own relevant checklist items individually, or upload using the csv template.
4. Assign checklist items to Task Owners and, **most importantly, set a review cycle** which triggers notifications to the task owners.
5. Assess your organisation's progress against each checklist item. (Not started; In progress; N/A; Complete)
6. Reset the residual risk level after you set your Status (in **5.**).

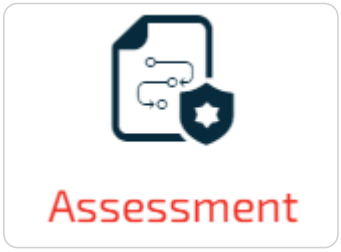


NOTE: By clicking the drop-down arrow on the right, the task owner can add audit notes and upload documents in support of the review.

Setting items to Complete in the Information Use & Security will also update the **Records of Processing Activities Report** which you will find under Governance.

BIG TIP: By clicking the white cross in the green circle, you may add your own sections and checklist items in each section. This feature is especially useful where you need to manage risks and issues you identify during the onboarding procedure or during normal operations.

Monitoring Compliance

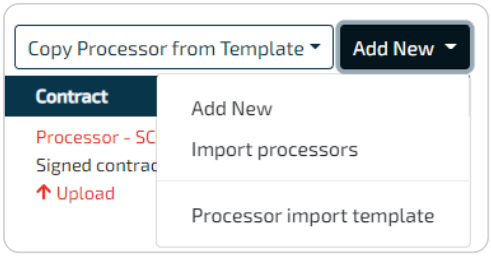


Run this report to keep track of and report on your compliance journey. Use the filter to target specific sections. Download the report in PDF or Excel format. It's good practice to regularly run and print the full report.

Processors

A Processor is a person/organisation that processes personal data on your behalf, under contract. They cannot use the personal data for their own purposes. An example would be a company that does payroll processing on behalf of your company.

Note that there is a Checklist. Go to Processor register. If you added any Processors in data mapping, they would appear here. This is where you maintain the Processor contracts. You could have uploaded your Processors here and they would have been available when you did your data mapping. You can add individually or by using the import template.

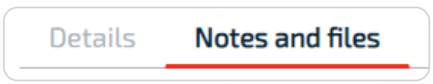


LGDP doesn't say *who* must draw up the contract, only that the Controller (your organisation) must ensure that the written contract stipulates the appropriate security measures that the Processor must establish and maintain. You might well find that some Processors already have the relevant contract *template*.

Edit the form **(1)** by completing the contact details, the contract start and end date. Set the status and Save the form. The status will display here **(2)**, Once you have the signed contract, upload it here **(4)**

You would have noticed that there is nothing under Lawful basis for our first Processor. That's because, in this example, they are based within the EU. However, the lawful basis in the second example **(3)** is 'SCCs – Exports ex EEA'. The link **(3)** takes you to the EDPB site that has the standard contractual clauses. will display a suggested template for BCRs. What is this about? – **it's important for you to understand Chapter V of LGDP** (or the relevant section in your Data Protection Act dealing with international transfers)

New feature – when you Edit a Processor you may now add Notes and Files to every Processor.



Data Sharing

Unlike the 'sharing' of personal data between Controller and Processor (which is under written contract), here we speak of the sharing (or, disclosure) of personal data *between Controllers*. An example might be the organisation providing medical insurance to your employees. In most cases there should already be some sort of agreement acknowledged between the two organisations. Simply upload a copy and set the status to Signed.

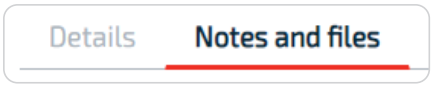
The functionality within the app is identical to the Processors section, except that the external links are relevant to controller-to-controller relationships.

It might help to look at a simple example.

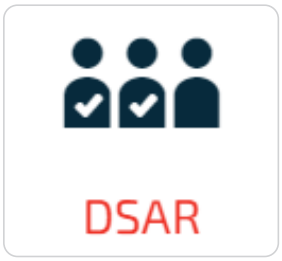
Let's say that a travel agent makes bookings on behalf of its clients with an airline and hotel chain. It's unlikely that the hotel chain and airline would be considered Processors. They are Controllers in their own right. But what if the three companies got together to develop a system or app that would be of value to ALL their clients? Now we're talking of *further* processing that brings about a **JOINT** sharing relationship – and will almost definitely require data subjects' consent. In fact, all the other Conditions (principles) come into play. It's important the data subject knows who to approach.

A more sophisticated and potentially, more-risky scenario of personal data sharing will be that of the world of data brokers.

New feature – when you Edit a Controller you may now add Notes and Files to every Controller.



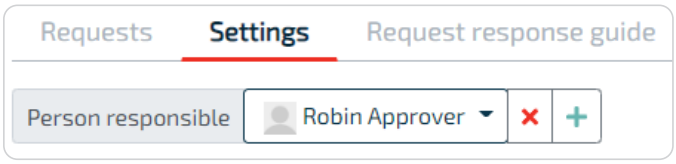
Data Subject Access Requests



There are several reasons why individuals might want to gain access to their personal data and several ways in which they can make these requests for access. Equally, there are several different responses that could come from your organisation.

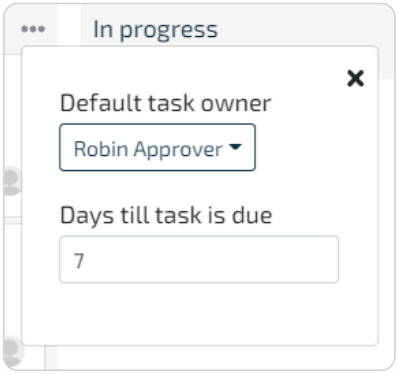
PrivIQ provides requesters with an online link and allows you to receive or capture the requests, delegate them as appropriate, navigate and understand the rules and gain oversight of progress via a dashboard.

Settings



Click Settings and set the 'Person responsible' for receiving online requests. If not in the drop-down, click the green cross to add new persons. The 'Person responsible' **must set the Notification Preference to be notified** when an online subject access request is received. To do this, click the drop-down under the username in the top right corner.

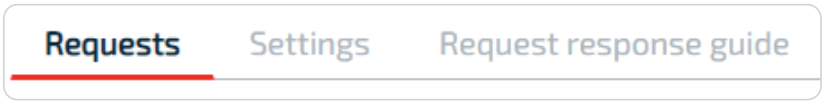
The 'Received' and 'In progress' sections have 3 dots. Set the default task owner and the number of days within which the default task owner must respond.



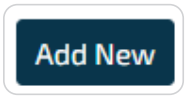
Online subject access request form

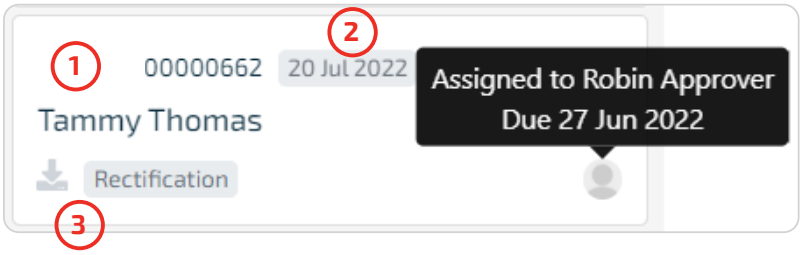
Still under Settings – ask your web developer to embed the code behind a link on your website – name it something relevant like 'Subject Access Requests'. Add the domains from where you will be calling this link. Click 'Preview' to see how it will present to the requester.

Requests

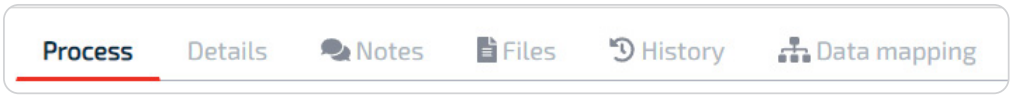


Online requests are auto-received here. You may add requests manually by clicking Add New



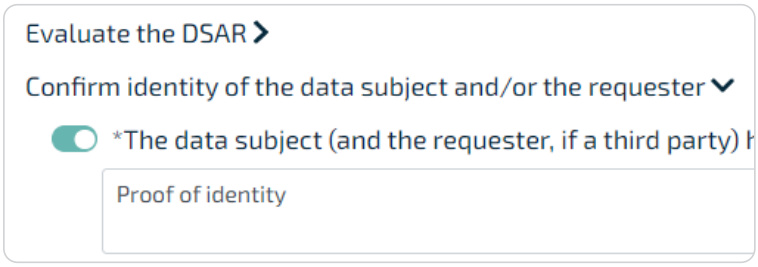


Looking at the panel above, we can see the automatically assigned reference number **(1)**, the due date **(2)** and the download button, **(3)**



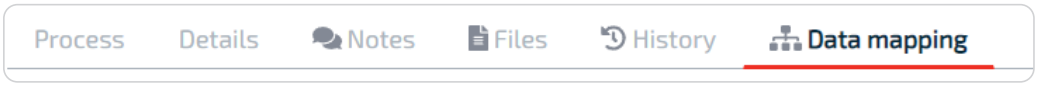
Click a panel to enter. When you click on Process you will notice the 3 stages – **Received, In Progress, and Complete.**

Received



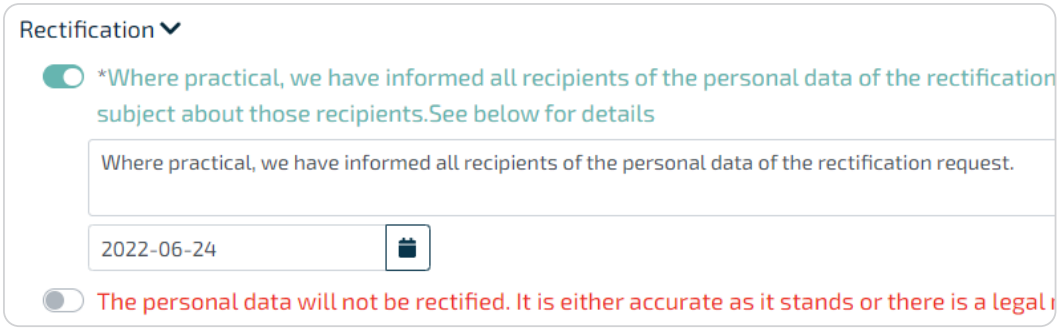
Evaluate the DSAR as there may be reasons why you wish to reject it. If it's a legitimate request, indicate how you have proven the identity of the requester. As soon as you tab out of that field, the Move to In Progress button is revealed.

In progress

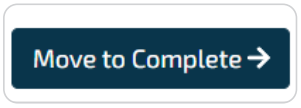


If your data mapping is accurate and current, it should give you clear indication of where to search. If you think any of the data mapping appears vague, inform your privacy manager. For example, if a processing location suggested 'Application Server', it might be useful to name the application instead.

Once you have all the data to support your decision, step through the rules. Any rule with a star * is mandatory. Hover over the text to see supporting information. The blue text indicates the request is successful and the red text means it has failed.



If you have followed the steps correctly, you'll be able to move the request to the Complete column.

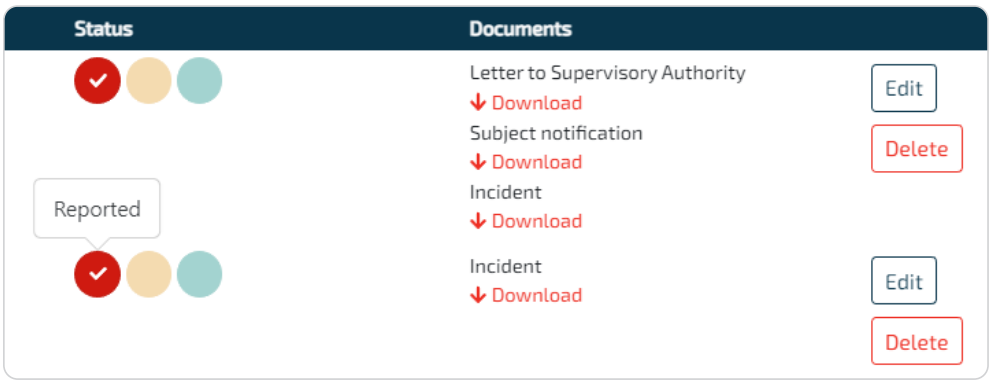


Breach Management

A personal data breach could lead to the accidental or unlawful use, destruction, loss, alteration, or disclosure of that information – in other words, a breach. A breach, not appropriately responded to, could result in physical, material, or non-material stress to data subjects and could well have a financial and/or reputational impact on your organisation.

A Controller must inform the Authority / Regulator as soon as reasonably possible after becoming aware of a security compromise. The Controller also needs to communicate with data subjects, especially where the exposure presents a high-risk to them. They should also consider the possibility that law enforcement authorities may need to be involved e.g., where there are safety concerns or perhaps, where early disclosure to data subjects could hamper investigations.

Use this section to capture and manage your responses to any incidents as well as communications with the Authority / Regulator and data subjects. Ensure that your Processors have a similar process in place. Doing table-top exercises fosters good practice that keeps the relevant staff aware of the processes involved in breach response management. Print those documents as evidence of training and then remove the incidents so that they don't obscure your dashboard.

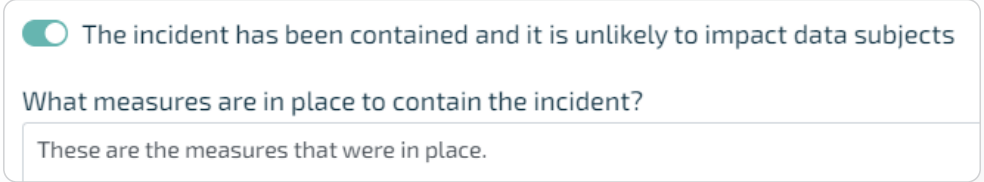


In the above example we have two types – the first where the incident was contained, there was no need to report it and we only needed the incident report. The second is where it had to be reported to both the Regulator and the data subjects impacted – in some cases you may be prevented from informing the data subjects.

Click Add New

Read the Introduction, followed by some background into Containment & Recovery.

Fill in the details required for the Incident title, followed by the Incident details. Next, we're at the Risk Assessment step.



Move to the final step which is the Incident evaluation and response. Clicking 'Finish' takes you back to the register and you will notice that it is only the Incident Report that is produced.

However, if the incident *hasn't* been contained you will move through the steps until you get Notification to the Authority / Regulator. Here you will find all the content which is based on your prior input. Use this information in your engagement with the Authority.

The next page is the content based on your prior input and should inform your communications with those data subjects who may be affected by the incident.

NOTE: Law enforcement – If you had selected this item under the Risk Assessment, the content you would normally use to communicate with data subjects will not be displayed.

Data Protection Impact Assessment

Conducting a DPIA is a legal requirement to help meet privacy and data protection expectations of customers, employees, and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project. This section allows you to identify why a DPIA is relevant for this project.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to individuals' resulting from the processing of personal data, by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help a controller to demonstrate that appropriate measures will be or have been taken to ensure compliance with LGDO.

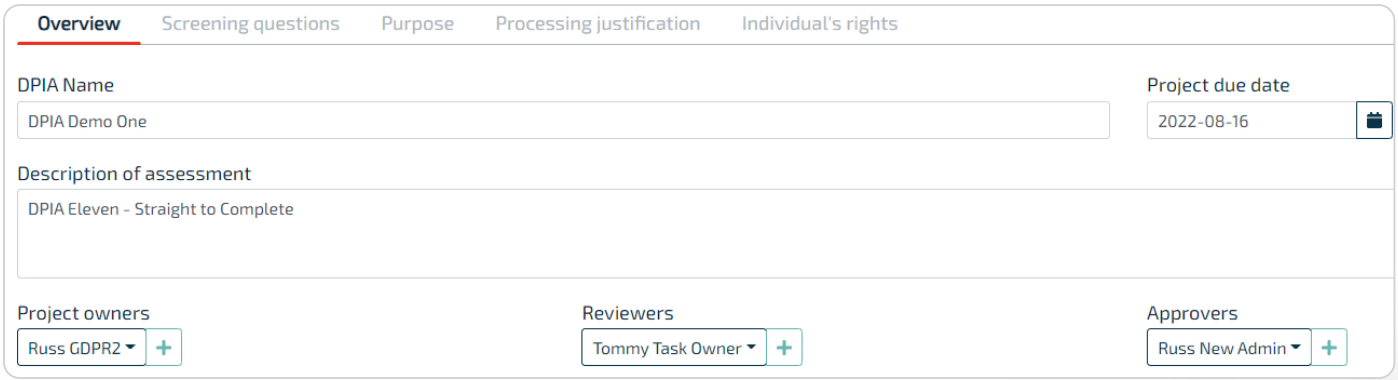
The EU's new Transfer Impact Assessment workflow is being added to the DPIA procedure and this document will be updated accordingly.

Some examples of where a DPIA may be required:

- A hospital processing its patients' genetic and health data
- The use of a camera system to monitor driving behaviour on highways. The data controller envisages to use an intelligent video analysis system to single out cars and automatically recognise license plates
- A company monitoring its employees' activities, including the monitoring of the employees' workstation, internet activity, etc
- The gathering of public social media profiles data to be used by private companies generating profiles for contact directories
- In some instances where the processing might require prior consultation with the Regulator

Click:

Enter the DPIA Name, Description and Project due date. Click **Save.**



The Project owner is usually the person compiling and editing the DPIA.

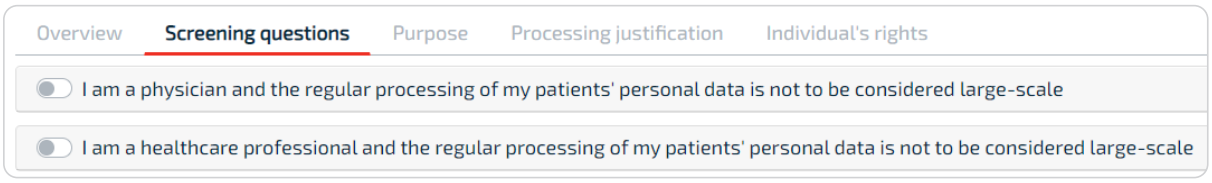
Select the **Reviewer**(s) or add any not in the drop-down list (click the green cross). Reviewers can only be Compliance Users or Task Owners.

Select the **Approver**(s). Approvers must be Administrator type users.

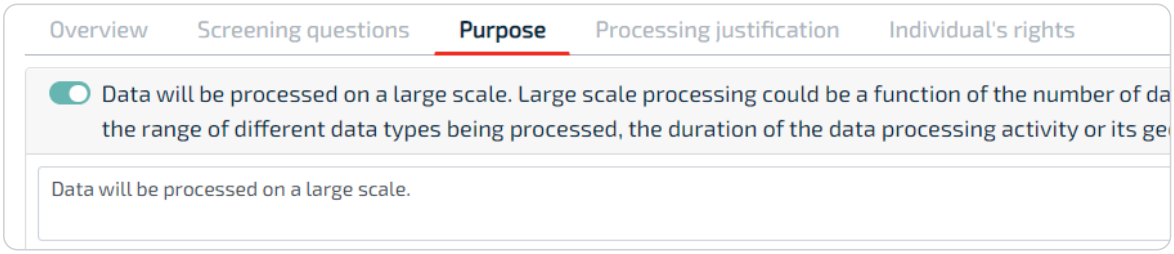
The DPO's comments in the DPIA will be recorded as such. Indicate which user is the DPO under Organisation/Users.

Screening Questions

By selecting an option under screening questions, you're suggesting that a DPIA is not relevant or required. The rest of the DPIA falls away. However, you still need to submit it for approval.

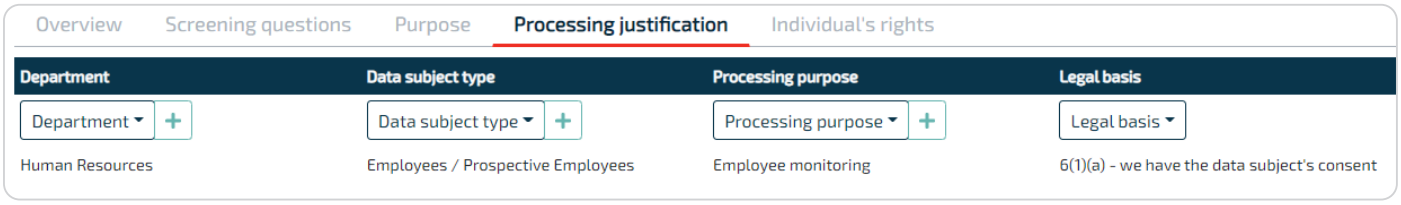


Purpose

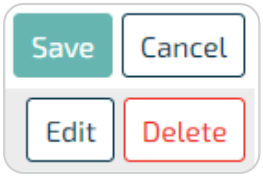


In this section, you indicate why the DPIA is relevant to this project or planned processing of personal data. Add comments or upload documents by clicking 'Notes and Files'. You may add your own reason for conducting a DPIA.

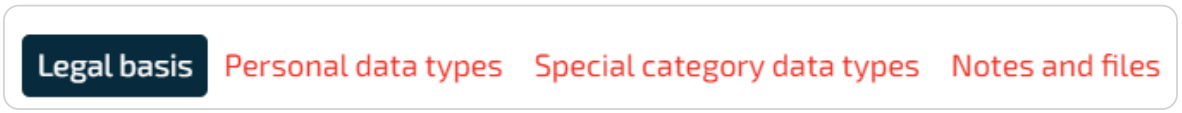
Processing justification



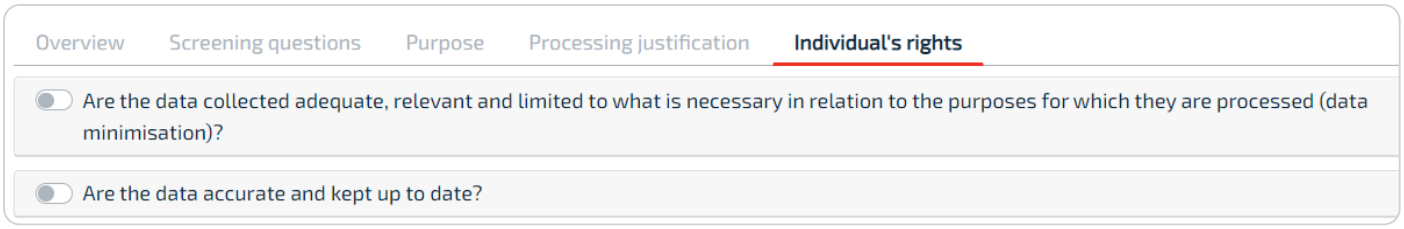
Select the relevant department / data subject type / processing purpose and legal basis. Then click **Save**.



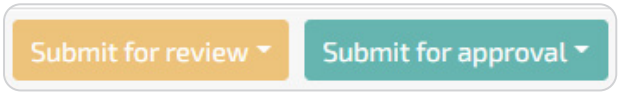
In the next panel, complete the mandatory fields (highlighted in red), enter the relevant personal data types, add any notes and files, and then click Close.



Individual's rights

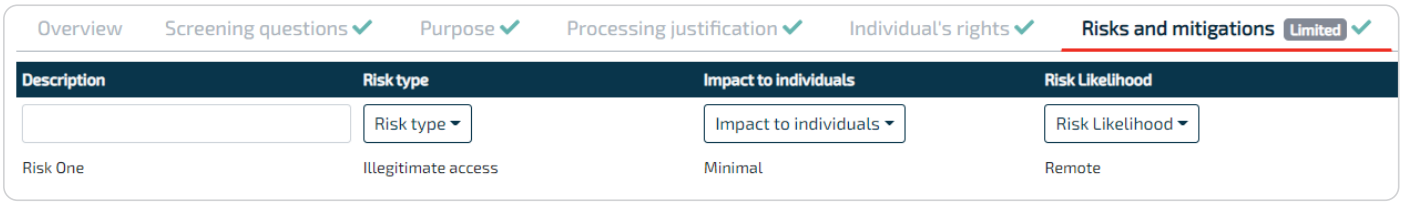


This section concerns data subjects' rights and **how those rights will be protected**. Once you have completed this section, you're now ready to submit the DPIA for Review (first) and for Approval (last). The reviewer and approver will receive notifications informing them of the task. After inserting their comments, the reviewer may return the DPIA for improvement or the Approver can approve the sections.



Risks and Mitigations

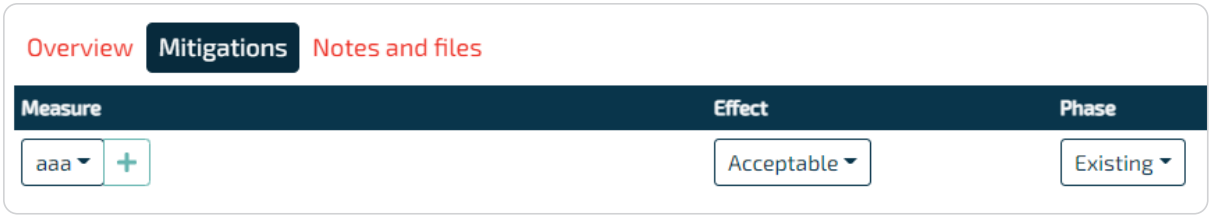
This then reveals the Risks and mitigations tab to the DPIA owner.



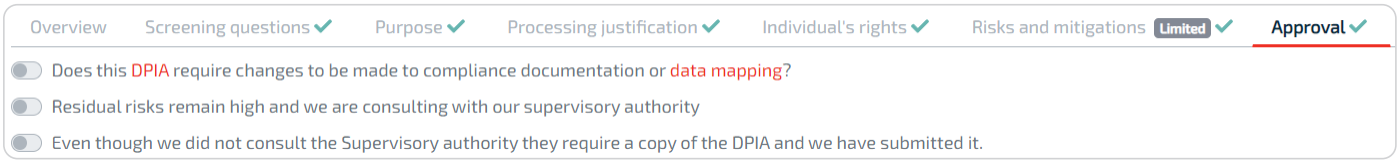
The DPIA owner will then add a relevant risk and click Save.

Then add an associated mitigation.

NOTE: If a mitigation has been added, it cannot be edited – it must be deleted and then replaced by the correct mitigation.

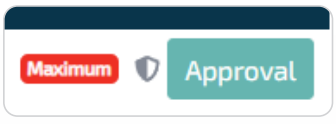


When all risks and mitigations are captured, submit the DPIA for approval.

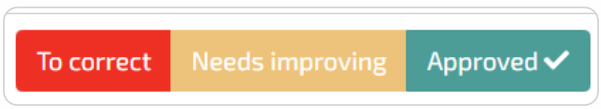


Final Approval

Approve each risk individually by clicking Approve to the right. Click Close and return to the main approval page.



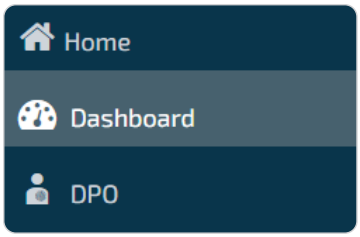
Then approve the risks overall by adding comments and the approval at the bottom of the page and submit to the owner.



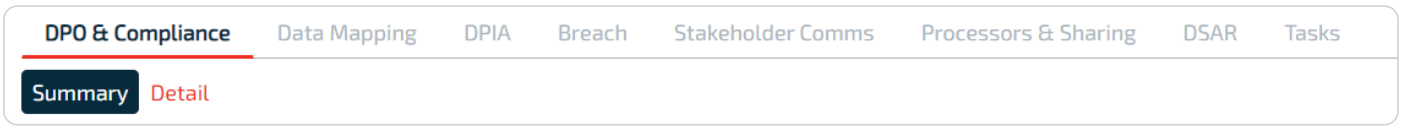
There are 2 possible outcomes after final approval. The owner could move the DPIA to Complete where those identified risks must be incorporated into your projects risk management framework. Or move it to the Submitted column where engagement with the Authority / Regulator is necessary.

Dashboard

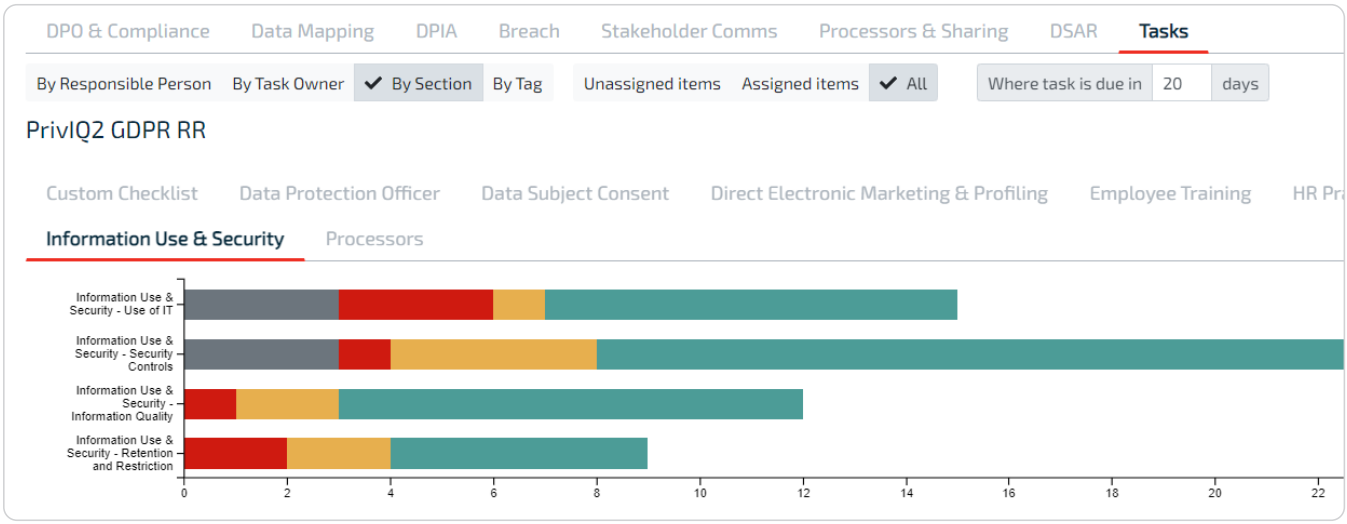
Find the dashboard icon in the sidebar.



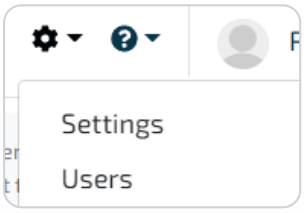
You may view across the various sections.



When you view tasks by task owner, click on the task owner to see which tasks have been assigned to the task owner.



User Maintenance



Add and manage users under Users. If you add Compliance Users here, you must ensure that they have been assigned as the person responsible in the relevant Compliance sections.

To provide an extra layer of security, we've added multi-factor authentication (MFA).

New users will receive a welcome email, inviting them to login with a temporary password and then changing their password. You can choose to either receive a verification code via SMS which you will enter along with password. Or, preferably, you can use an authenticator, such as Authy, Google Authenticator (iOS/Android) or Microsoft Authenticator, that will generate the verification code to enter with your password.