TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de empresa especializada no fornecimento do sistema de gestão integrada referente à LGPD, por meio de sistema informatizado, utilizando plataforma em nuvem (SAAS), incluindo gestão do consentimento, Gestão de Projetos de Privacidade, Gestão de Incidentes, Gestão de Políticas, Pedidos dos Titulares, Data Discovery, Data Mapping, nos termos detalhados no corpo do presente Termo de Referência.

2. JUSTIFICATIVA

2.1. A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também tem como foco a criação de um cenário de segurança jurídica, com a padronização de regulamentos e práticas para promover a proteção aos dados pessoais.

2.2. De acordo com o seu artigo 50, os controladores de dados pessoais poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

2.3. Com efeito, vale ressaltar que a melhor maneiro de se estabelecer todas essas práticas apresentadas pela norma é por meio de ferramentas digitais que auxiliem aos gestores no seu dia a dia, e no processo de tomada de decisão.

3. ESPECIFICAÇÕES DO OBJETO

3.1. O canal LGPD deverá ser eficaz e atrativo devendo possuir as estruturas mínimas abaixo estabelecidas:

3.1.1. A solução tecnológica deverá ser disponibilizada no modelo Software como Serviço (SaaS), ou seja, pronta para utilização pela CEDAE, sendo transparentes para o Contratante toda e qualquer questão tecnológica ou de infraestrutura relacionada à efetiva disponibilização da ferramenta, que será acessada via Internet (em nuvem).

3.1.2. A solução tecnológica deverá ter capacidade para permitir a sua utilização por inúmeros usuários, tanto do lado da CEDAE quanto do lado do Titular de Dados, em regime de 24 horas por dia e 07 dias por semana. A infraestrutura de nuvem deverá ser robusta e segura o suficiente para permitir, inclusive, inúmeros acessos simultâneos.

3.1.3. Identificação dos titulares de dados: a contratada deverá identificar os titulares de dados com, no mínimo, Nome, CPF ou matrícula da CEDAE.

3.1.4. A CONTRATADA deverá firmar termo de confidencialidade, por seus administradores, empregados, prepostos e contratados, obrigando-se a manter o mais completo e absoluto sigilo em relação a toda e qualquer informação a que tenham acesso, não podendo, sob qualquer pretexto, utilizá-las para si, divulgar, reproduzir ou delas dar conhecimento a terceiros, inclusive após o término da prestação de serviços.

3.2. Suporte Técnico e Update de Versão

3.2.1. O serviço de update de versão se refere ao fornecimento de novas versões e releases dos produtos da solução lançados no decorrer da vigência do contrato. A cada nova liberação de versão e release, a CONTRATADA deverá disponibilizar em pleno uso, as atualizações, os manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas.
3.2.2. As licenças incluem garantia de update para novas versões, tanto corretivas quanto evolutivas, durante o período do contrato, sem custo adicional a CEDAE.
3.2.3. O suporte técnico remoto poderá ser solicitado por meio de abertura de chamados, acesso a portais Web de suporte da contratada, correio eletrônico e ligações telefônicas.
3.2.3.1. Este serviço destina-se à prestação de suporte remoto ao uso e à resolução de ocorrências relacionadas ao funcionamento inadequado, inesperado ou dúvidas sobre a utilização do produto fornecido, de acordo com suas especificações técnicas.

3.3. Configurações Gerais e Segurança

3.3.1. O sistema de gestão da privacidade deve ser acessível através dos navegadores de internet mais populares, em suas versões mais atualizadas, como: Google Chrome, Microsoft Edge, Mozilla Firefox, sem limitações ou exigência de plugins ou complementos para sua plena execução.
3.3.2. O sistema deve funcionar em protocolo HTTPS para todas as requisições.
3.3.3. Deve ser possível configurar permissões de acesso e perfis com determinadas permissões conforme preferência do administrador.
3.3.1. Deve possuir Workflow nativo sem necessidade de software de terceiros.
3.3.1.1. O workflow permitirá automatizar fluxos e executar um conjunto discreto de atividades com suporte a papeis, condições transacionais e temporais (deadlines).
3.3.1.2. Parametrização do workflow será através de modelagem visual.
3.3.2. O sistema deve permitir autenticação através do protocolo SSO com Azure utilizando SAML.
3.3.3. Deve ser possível configurar o provedor de envio de e-mails através de protocolo SMTP com criptografia TLS/SSL para notificação de alertas e mensagens do sistema.
3.3.4. O software deve funcionar, sem limitações, no idioma português do Brasil, com exceção de palavras e termos comuns da língua inglesa como “mouse”.
3.3.5. A plataforma deve possuir manual para operação em idioma português do Brasil.
3.3.5.1. Toda e qualquer documentação, manuais, inclusive de APIs e integrações, devem estar disponíveis no idioma português do Brasil.
3.3.6. Além dos manuais, a plataforma deve ter treinamentos em português do Brasil para que possa ser aplicado para todos os usuários.
3.3.7. Deve permitir acesso através de dispositivos móveis como tablets e celulares através do navegador de internet, podendo ser realizado através de Interface responsiva: adaptável ao dispositivo.
3.3.8. Deve possuir trilha de auditoria com todas as ações e eventos que um determinado usuário do sistema realizou. O log deve persistir na ferramenta em tempo não inferior a 12 meses do evento gerador.
3.3.9. Deve ser possível configurar determinado usuário(s) como sendo o DPO (Encarregado) da organização.
3.3.10. O sistema deve permitir relacionar áreas de negócio, cargo e funções para um usuário do sistema.
3.3.11. Deve permitir configurar o tempo de timeout (encerramento da sessão) dos usuários conectados na plataforma.
3.3.12. O sistema deve ter, em um local centralizado, todas as tarefas do projeto de adequação. As tarefas podem ser cadastradas em diferentes módulos do sistema.

3.3.13. Deve ter possibilidade de configurar a quantidade máxima de tentativas de login na plataforma, este deve ser protegido por Captcha.
3.3.14. O sistema deve possuir a opção de recuperar a senha: "esqueci minha senha".
3.3.15. A senha dos usuários deve expirar após um determinado número de dias, configurável pela plataforma. Que deverá obedecer às regras definidas através do AD da CEDAE.
3.4. O sistema deve permitir que se configure a quantidade máxima de dias que um determinado usuário pode ficar sem autenticar-se na ferramenta, antes de ser automaticamente bloqueado.
3.4.1. Todos os módulos e recursos devem fazer parte da mesma plataforma e fabricante.
3.4.2. API - Todos os serviços (API) que a plataforma disponibiliza devem utilizar meios seguros, através de criptografia.
3.4.3. As credenciais de autenticação devem poder ser gerenciadas pelo administrador do sistema através da interface web.

3.5. Monitoramento de Sites

3.5.1. O sistema deve realizar o monitoramento de websites da CEDAE (Intranet e Internet) para identificar falhas, riscos de privacidade e outros critérios e verificações aqui especificadas.
3.5.2. Permitir o cadastro de websites para monitoramento sem limitação de quantidade de domínios.
3.5.3. Para cada website cadastrado exigir a verificação de propriedade do domínio do website através de DNS ou conferência de arquivo hospedado no website;
3.5.4. Permitir informar uma periodicidade de recorrência do monitoramento automático.
3.5.5. Quando informada a periodicidade deve exibir a data agendada da próxima execução automática do monitoramento.
3.5.6. Exibir relatório técnico para que a área de tecnologia possa tomar providências quanto ao resultado do monitoramento.
3.5.7. Exibir relatório não-técnico para que a área de negócios possa tomar providências quanto ao resultado do monitoramento.
3.5.8. O monitoramento deve avaliar no mínimo os seguintes critérios, apresentando resultados em sistema web.
3.5.8.1. Existência de tratamento de dados sensíveis;
3.5.8.2. Validar se respeita o princípio da necessidade da coleta para o tratamento de dados pessoais;
3.5.8.3. Validar se a finalidade da coleta está bem definida para cada tratamento de dado pessoal;
3.5.8.4. Verificar o uso excessivo de recursos do navegador como “local Storage”, “banco de dados”, “cookies”, “scripts” e “plugins”
3.5.8.5. Validar a existência de compartilhamento de dados pessoais com terceiros;
3.5.8.6. Verificar se todas as páginas estão sendo tratadas em um canal seguro de criptografia ponta-a-ponta;
3.5.8.7. Exibir a lista de formulários, campos e classificação de risco para cada campo que represente um dado pessoal;
3.5.8.8. Exibir a lista de todos os identificadores eletrônicos (cookies) encontrados e seus metadados.
3.5.9. Permitir indicar um endereço de e-mail para envio de notificações quando um monitoramento completar a sua execução.
3.5.9.1. O e-mail com a notificação deve possuir um relatório resumido da varredura realizada.
3.5.10. Deve permitir sincronizar o monitoramento com a gestão de cookies para sempre exibir os cookies mais atualizados na plataforma de gerenciamento de cookies.
3.5.11. Deve permitir visualizar e navegar pelos monitoramentos anteriores (histórico de monitoramento) para poder comparar os resultados.
3.5.12. O sistema deve permitir o cadastramento de domínios extras, vinculados ao website, como no caso de subdomínios.

3.6. Gestão de Cookies

3.6.1. Permitir o cadastro de grupos de cookies de modo que possam ser exibidos em categorias.
3.6.2. Permitir ordenar os grupos de cookies com facilidade, utilizando recursos como “drag and drop”.
3.6.3. Permitir definir um ou mais grupos de cookies como sendo “Obrigatórios” de modo que os cookies pertencentes a este grupo não irão solicitar consentimento do usuário.
3.6.4. Permitir agrupar cada cookie importado pelo “Monitoramento de sites” em um dos grupos registrados.
3.6.5. Permitir registrar novos cookies manualmente e agrupá-los em um dos grupos registrados.
3.6.6. Permitir gerenciar os metadados de cada cookie com, no mínimo, os seguintes atributos:
3.6.6.1. Nome do cookie
3.6.6.2. Host do cookie
3.6.6.3. Tipo de cookie (Persistente ou de Sessão)
3.6.6.4. Finalidade do cookie
3.6.7. Permitir que o administrador configure as propriedades visuais de cada janela, sem precisar conhecer linguagem de programação, de forma fácil e prática com, no mínimo, as seguintes possibilidades:
3.6.7.1. Alteração do título e descrição da janela;
3.6.7.2. Alteração das cores (fundo, borda, fonte, botões);
3.6.7.3. Inserção de links externos;
3.6.7.4. Controle de botões e seus textos;
3.6.7.5. Exibição de botão para fechar o banner, aceitar os cookies ou rejeitar os cookies;
3.6.7.6. Controle de conteúdo adicional com informações úteis para o usuário final (texto livre).
3.6.7.7. Inserção dinâmica de código CSS (folhas de estilo) para personalização mais técnica, utilizando interface WYSIWYG.
3.6.8. O administrador poderá optar em realizar o registro de logs de consentimentos de modo que cada consentimento registrado pelo usuário irá registrar um evento para análise e acompanhamento da administração.
3.6.9. Deve permitir exibir para o administrador os logs de eventos de consentimento com, no mínimo, as seguintes informações:
3.6.9.1. Identificador anonimizado da origem da coleta;
3.6.9.2. Ação realizada pelo usuário (Aceitação de cookies, Rejeição de cookies, Aceitação de Grupos de cookies, Rejeição de Grupos de cookies, Aceitação de todos os cookies, Rejeição de todos os cookies)
3.6.9.3. Data e hora da ocorrência.
3.6.9.4. IP e dados do navegador do usuário (se habilitado esse tipo de coleta pelo administrador).
3.6.10. Deve permitir que o administrador faça filtros no controle de logs de eventos de consentimento.
3.6.11. Deve exibir uma lista de todos os links de script (JavaScript) importados pelo módulo de “monitoramento de sites” e permitir que o administrador faça o vínculo de cada script com os seus cookies possíveis.
3.6.12. Deve permitir a geração de um código da janela para inserção no código-fonte do website de modo a exibir a janela de consentimento de cookies para o público final.
3.6.13. Deve permitir realizar o bloqueio de cookies de dois modos: Automático e Manual.
3.6.13.1. Bloqueio automático: apenas a inserção do código no website é suficiente para que todos os cookies dos grupos “não obrigatórios” sejam bloqueados, ou seja, sem a necessidade de programação adicional.
3.6.13.2. Bloqueio manual: a inserção do código no website combinado com eventuais mudanças na estrutura do código-fonte do website é necessária para que todos os cookies dos grupos “não obrigatórios” sejam bloqueados.

3.6.14. Deve permitir exibir a janela de controle de consentimento nos websites vinculados.
3.6.15. Deve permitir que o usuário final faça a escolha entre aceitar ou rejeitar cookies com no mínimo as seguintes opções:
3.6.15.1. Aceitar todos os cookies.
3.6.15.2. Rejeitar todos os cookies.
3.6.15.3. Aceitar grupos de cookies específicos.
3.6.15.4. Rejeitar grupos de cookies específicos.
3.6.15.5. Aceitar um cookie específico.
3.6.15.6. Rejeitar um cookie específico.
3.6.16. O sistema deve permitir que se faça uma gestão de conteúdos adicionais na janela de cookies para exibição de políticas e termos de uso, por exemplo.
3.6.16.1. As políticas podem ser escritas pelo administrador da plataforma na própria ferramenta de cookies.
3.6.16.2. O sistema deve poder importar políticas já escritas anteriormente.
3.6.17. Quando o administrador do sistema alterar qualquer finalidade de um cookie ou o sistema adicionar novos cookies, os usuários que aceitaram ou recusaram os cookies anteriormente devem ser questionados novamente ao voltar ao website.
3.6.18. Deve ser possível relacionar finalidades de tratamento de dados pessoais com categorias de cookies.

3.7. Gestão de Políticas

3.7.1. Permitir a gestão de políticas para cada website cadastrado e que se possa definir políticas comuns para todos os websites.
3.7.2. Deve permitir o versionamento de políticas e suas alterações.
3.7.3. Deve permitir criar políticas privadas (internas) ou políticas públicas (com link aberto acessível ao público).
3.7.4. Deve permitir a edição das políticas em formato aberto (HTML) para aplicações na internet.
3.7.5. Deve permitir imprimir a política em PDF.
3.7.6. Deve permitir o controle de revisões onde um usuário pode enviar para outro usuário registrado no sistema para revisão da política, que ficará pendente aprovação.
3.7.7. O sistema deve permitir o gerenciamento de múltiplos leiautes de políticas.
3.7.8. Deve permitir agregar uma área para coleta do consentimento do usuário em uma determinada política utilizando o módulo de gestão do consentimento.
3.7.9. Deve ser possível enviar uma política para aprovação de outro usuário cadastrado.
3.7.10. O sistema deve permitir que o usuário visitante, navegue por todas as versões da política publicada.
3.7.11. O sistema deve permitir que o usuário visitante, faça uma comparação visual das mudanças que foram feitas entre versões diferentes de uma política.
3.7.12. Deve ser possível conferir os consentimentos/atestamentos em uma política através de relatórios no sistema.

3.8. Gestão do Consentimento

3.8.1. A plataforma deve possuir uma gestão de dados dos titulares identificados com, no mínimo, os seguintes atributos:
3.8.1.1. Nome.
3.8.1.2. E-mail.
3.8.1.3. Matrícula CEDAE.
3.8.1.4. Documento de identificação (CPF, CNPJ).
3.8.1.5. Telefone.
3.8.1.6. Origem ou sistema (sistema que originou o cadastro).
3.8.2. A plataforma deve oferecer gestão visual de todos esses titulares e fácil acesso aos seus consentimentos registrados.
3.8.3. A plataforma deve permitir a busca por um Documento, e-mail e por matrícula CEDAE do usuário de forma fácil.
3.8.4. Deve permitir o cadastro de finalidades de consentimento e agrupá-las por categorias.
3.8.5. Deve possuir controle de tempo máximo de retenção do consentimento de modo que a ferramenta faça a revogação do consentimento automaticamente após expiração da data.
3.8.6. Para cada finalidade de consentimento deve permitir a inclusão de um ou mais atributos (dados pessoais) que serão coletados por essa finalidade.
3.8.7. Deve permitir criar links para redirecionar o usuário que concedeu ou revogou um determinado consentimento.
3.8.8. Deve possuir uma área de testes para que o administrador possa garantir o funcionamento da coleta de consentimentos antes de utilizá-la em seus sistemas.
3.8.9. A plataforma deve permitir que se faça um filtro por titulares que concederam e/ou revogaram consentimentos de determinadas finalidades de processamento.
3.8.10. A plataforma deve possuir uma API para integração entre sistemas com documentação em português do Brasil.
3.8.11. Deve ser possível cadastrar aplicativos para terem um controle de consentimentos.
3.8.12. Deve permitir o controle das permissões a serem gerenciadas no aplicativo através de um sistema web onde cada permissão permite a escrita da sua finalidade para o usuário final.
3.8.13. Deve permitir que o usuário final habilite ou desabilite as permissões no aplicativo através da interface do controle de privacidade.
3.8.14. Deve possuir dashboard de consentimentos com dados e estatísticas
3.8.15. Deve permitir que o operador do sistema faça a revogação ou aceite de consentimentos em nome de um titular para casos em que o titular não tenha como fazer a ação livre de consentimento.
3.8.15.1. No caso de registros feitos por operadores do sistema, a plataforma deve guardar todos os logs para auditoria da ação realizada.
3.8.16. Deve permitir vincular uma finalidade de consentimento com os registros das operações de tratamento (ROPA).
3.8.17. O sistema deve ter um relatório sintético de finalidades onde seja possível ver quantos consentimentos positivos ou negativos foram coletados para cada finalidade.
3.8.18. Se o administrador do sistema alterar uma finalidade, os usuários que aceitaram ou recusaram essa finalidade devem ser questionados novamente para atualizar o seu consentimento.
3.8.19. O sistema deve possuir um local para gerar um QRCODE para coleta de consentimentos que pode ser usada em atendimentos presenciais ou para enviar por canais digitais.
3.8.20. Como podem ter várias dezenas de funcionários coletando consentimentos em diferentes pontos de atendimento, o sistema deve a coleta de consentimentos com poucos cliques, sem que o funcionário precise estar conectado no sistema web.
3.8.21. O sistema deve enviar o pedido ou renovação de consentimentos de titulares por e-mail:
3.8.21.1. Deve permitir a criação de campanhas para envio por e-mail sem limitação do número de pessoas ou e-mails enviados.

3.8.21.2. Deve existir um local para configurar os templates (modelos) de e-mails que serão enviados.
3.8.21.3. O administrador deve conseguir segmentar os titulares para criar diferentes segmentações e critérios para envio de e-mail pedindo consentimentos.
3.8.21.4. O administrador deve conseguir relacionar diferentes finalidades de tratamento de dados para justificar a coleta do consentimento.

3.9. Pedidos dos Titulares

3.9.1. Deve ser possível gerenciar os pedidos dos titulares de dados pessoais.
3.9.2. Deve ser possível gerenciar as fases de atendimento do pedido e seus respectivos prazos de atendimento.
3.9.3. Deve ser possível gerenciar o template de e-mails trocados entre o controlador e o titular do dado pessoal.
3.9.4. Os templates de e-mail devem suportar o padrão HTML e a plataforma deve oferecer guias e variáveis para que o administrador possa personalizar o e-mail.
3.9.5. Deve ser possível gerar um link do formulário de atendimento para inclusão em websites com o formulário de atendimento dos titulares de dados pessoais.
3.9.6. Deve permitir gerar links para o formulário de atendimento já pré-configurado em um determinado idioma.
3.9.7. Deve oferecer ao titular dos dados pessoais, no mínimo, os seguintes direitos:
3.9.7.1. Confirmação da existência de tratamento.
3.9.7.2. Correção de dados.
3.9.7.3. Portabilidade de dados.
3.9.7.4. Acessar meus dados.
3.9.7.5. Remover todos os meus dados.
3.9.8. O idioma da ferramenta do usuário final é português do Brasil.
3.9.9. Deve ser possível anonimizar os dados do titular uma vez o atendimento seja concluído conforme critério do controlador.
3.9.10. Deve ser possível responder o pedido do titular.
3.9.11. Deve oferecer interfaces de integração para outros sistemas através de padrões e protocolos conhecidos de mercado.
3.9.12. Deve ser possível inserir anotações privadas no atendimento do pedido.
3.9.13. Deve exibir um mecanismo de controle de segurança AntiSpam (Captcha) no formulário público de atendimento.
3.9.14. Deve permitir configurar um endereço de e-mail para receber as notificações de novos pedidos.
3.9.15. O titular que fez um pedido deverá receber um e-mail para confirmar a sua identidade com um link seguro de confirmação.
3.9.16. A plataforma deve permitir personalizar, de forma fácil, a tela de confirmação com, no mínimo, as seguintes propriedades:
3.9.16.1. Ícone indicando o sucesso da confirmação.
3.9.16.2. Cor de fundo da página.
3.9.16.3. Cor de fundo da área de conteúdo.
3.9.16.4. Mensagem de sucesso e sua respectiva cor de fonte.
3.9.16.5. Mensagem customizada e sua respectiva cor de fonte.
3.9.17. A plataforma deve permitir que o titular envie um arquivo em anexo na sua solicitação.
3.9.18. A plataforma deve permitir que o responsável responda a solicitação do titular anexando um arquivo.
3.9.19. A plataforma deve permitir realizar filtros por atributos comuns de atendimentos com, no mínimo, as seguintes propriedades:

3.9.19.1. Protocolo de atendimento.
3.9.19.2. Datas de criação e de expiração.
3.9.19.3. Nome do titular solicitante.
3.9.19.4. Tipo de direito solicitado.
3.9.19.5. Fase de atendimento.
3.9.20. Deve exibir em uma tela de atendimento todo o histórico de interações com o titular, desde todas as respostas até anotações e trilhas de auditoria.
3.9.21. Deve registrar em trilhas de auditoria todas as mudanças e eventos de um atendimento.
3.9.22. O sistema deve permitir que a empresa crie portais para atendimento dos titulares, sem limite de quantidade com, no mínimo, as seguintes configurações possíveis:
3.9.22.1. Alteração de logotipo, cores e layout.
3.9.22.2. Permitir mudanças no CSS para cada portal.
3.9.22.3. Personalização avançada do HTML do portal.
3.9.22.4. Permitir o cadastramento e alteração de dados de titulares.
3.9.22.5. Permitir exclusão de titulares no portal.
3.9.22.6. Exibir todos os pedidos do titular logado.
3.9.22.7. Permitir que o titular responda os pedidos.
3.9.22.8. Permitir que o titular veja o prazo de atendimento nos seus pedidos.
3.9.22.9. Garantir que o titular consiga ver todos os seus consentimentos aceitos e revogados.
3.9.22.10. Garantir que o titular consiga modificar o seu consentimento de forma livre.
3.9.22.11. Garantir que o titular consiga encerrar um pedido criado anteriormente.
3.9.22.12. Permitir que o titular consulte o status de um pedido através do protocolo e e-mail, sem precisar autenticar.
3.9.23. O sistema deve ter um local onde o operador do sistema possa criar pedidos em nome de titulares para ser usado nos casos em que o titular esteja impossibilitado de exercer seu direito em um canal digital. O sistema deve registrar o usuário que criou o pedido em nome do titular de dados.
3.9.24. Deve ser possível definir agentes (funcionários) responsáveis por um determinado pedido de titular.
3.9.25. O formulário de pedidos dos titulares deve poder ser customizado com novos campos a qualquer momento:
3.9.25.1. Para cada novo campo deve ser possível definir uma expressão regular de validação.
3.9.25.2. Para cada novo campo deve ser possível definir uma dependência com outro campo.
3.9.26. Deve ser possível vincular tarefas relacionadas a um pedido de um titular de modo que outras pessoas do time possam trabalhar no atendimento.
3.9.27. O sistema deve apresentar um relatório sintético de atendimentos realizados mês a mês com, no mínimo, os seguintes filtros: Pedido recebidos, Respostas feitas, Pedidos sem resposta, Respostas do titular, Expiração de prazo.
3.9.28. O sistema de atendimento aos titulares deve ter integração nativa com o módulo de descoberta de dados pessoais (Data Discovery) de modo que um pedido que chegue possa ter seu atendimento automatizado.

3.10. Data Mapping (Mapeamento de dados)

3.10.1. Deve permitir a gestão dos pontos de coleta de dados pessoais.
3.10.2. A gestão dos pontos de coleta de dados pessoais deve ser relacionada aos websites da CEDAE.
3.10.3. Deve permitir o cadastramento de vários tipos de pontos de coleta como: banco de dados, API, formulários web, entre outros meios digitais.
3.10.4. Deve possuir sistema para registro de operações de tratamento de dados (ROPA), sem limitações.
3.10.5. Deve ser possível agrupar as operações de tratamento (ROPA) para facilitar a organização.

3.10.6. O cadastro do fornecedor deve permitir informar os contatos com o encarregado pelo tratamento de dados pessoais.
3.10.7. O sistema deve permitir que relatórios e dados de *due diligence* (diligência prévia) sejam anexados.
3.10.8. Deve permitir vincular uma entidade de tratamento de dados pessoais.
3.10.9. Deve permitir o cadastro de dados pessoais dentro de uma atividade de tratamento de dados.
3.10.10. Deve permitir vincular metadados diversos *(tags)* às operações de tratamento com "chave=valor".
3.10.11. Deve permitir a gestão de riscos relacionados a cada ROPA com, no mínimo, as seguintes propriedades de controle:
3.10.11.1. Nível do risco.
3.10.11.2. Categoria de risco.
3.10.11.3. Ameaça.
3.10.11.4. Vulnerabilidade.
3.10.11.5. Controles e Normas.
3.10.11.6. Informações sobre a ameaça e vulnerabilidades.
3.10.11.7. Plano de tratamento do risco.
3.10.11.8. Data da solução.
3.10.11.9. Usuário responsável pela mitigação e tratamento do risco.
3.10.12. O administrador deve poder personalizar novas ameaças, vulnerabilidades, controles e categorias.
3.10.13. O sistema deve permitir que o administrador crie modelos de riscos prontos e reutilize estes modelos quando for atribuir um novo risco.
3.10.14. O sistema deve sugerir possíveis riscos no ROPA conforme o preenchimento do mesmo vai acontecendo.
3.10.15. Deve permitir cadastrar atributos (dados pessoais) vinculados ao ROPA.
3.10.16. Deve permitir informar se um dado pessoal é relacionado a criança ou adolescente.
3.10.17. Deve permitir cadastrar transações e fluxos de dados com, no mínimo, as seguintes propriedades:
3.10.17.1. Direção da transação (saída de dados ou entrada de dados).
3.10.17.2. Entidade de tratamento de dados de origem.
3.10.17.3. Entidade de tratamento de dados de destino.
3.10.17.4. Quantidade média de dados afetados pela transação.
3.10.17.5. Volume de dados transacionados.
3.10.17.6. Seguranças empregadas na transação.
3.10.18. Deve permitir um trabalho de classificação e mapeamento de tratamento de dados pessoais para cada atributo de cada ROPA registrado.
3.10.19. Deve permitir informar para cada atributo no mínimo as seguintes informações relacionadas com o fluxo de tratamento de dados pessoais:
3.10.19.1. Validação se é um dado identificado ou identificável.
3.10.19.2. Validação se é um dado sensível e um dado obrigatório.
3.10.19.3. Aspectos de criptografia e segurança do dado.
3.10.19.4. Aspectos de auditoria e logs do dado.
3.10.20. Deve permitir o registro das finalidades de processamento para cada dado pessoal e para cada operação de tratamento.
3.10.21. Deve permitir cadastrar categorias de dados pessoais (atributos) para melhor classificá-los.
3.10.22. O controle de finalidades de processamento deve prever todas as hipóteses de tratamento de dados pessoais da LGPD.
3.10.22.1. No caso da hipótese de tratamento "Consentimento" deve ser viável realizar um controle adicional para justificar o uso dessa hipótese.
3.10.23. Deve possuir ferramentas de controle quanto à remoção de dados pessoais para orientar o controlador quanto aos riscos dessa ação.

3.10.24. Deve ser possível visualizar de modo gráfico o ciclo de vida dos dados pessoais dentro da organização.
3.10.25. Deve possuir um cadastro de regulamentações para uso no mapeamento de dados quanto aos aspectos regulatórios
3.10.26. Deve ser possível criar modelos de classificação de atributos para poder reutilizar um modelo em um novo atributo
3.10.27. O Sistema deve gerar automaticamente o DPIA (RIPD) - Relatório de Impacto de Proteção de Dados) para uma ou mais atividades de processamento conforme escolha do usuário.
3.10.28. O sistema deve permitir a impressão do relatório de impacto gerado.
3.10.29. Deve ser possível vincular tarefas relacionadas a uma operação de tratamento de modo que outras pessoas do time possam trabalhar na adequação.
3.10.30. A plataforma deve ter um relatório de temporalidade de modo a exibir, em uma única tela, todos os dados pessoais e seu prazo de retenção para o devido controle do prazo de processamento do dado.
3.10.31. A plataforma deve ter um relatório sintético de bases legais que mostre a quantidade de operações de tratamento, quantidade de dados pessoais e quantidade de dados pessoais sensíveis para cada base legal da LGPD.
3.10.32. A plataforma deve possuir uma representação visual/gráfica de todo o ciclo de vida dos dados pessoais de uma determinada operação de tratamento, evidenciando a coleta, tratamento, distribuição e remoção de dados.
3.10.33. A plataforma deve permitir a exportação do ROPA em Excel e PDF de um ou vários processos.

3.11. Integrações

3.11.1. O sistema deve permitir a criação de conectores web para que sejam chamados quando determinados eventos acontecerem.
3.11.2. Deve ser intuitivo para o operador da plataforma a criação de conectores sem que seja necessária qualquer programação de software adicional à existência do próprio serviço de destino.
3.11.3. Os eventos que devem gerar rotinas de integração devem ser no mínimo:
3.11.3.1. Quando um novo titular é registrado na plataforma.
3.11.3.2. Quando um novo pedido de titular é registrado.
3.11.3.3. Quando um pedido de titular possui mudança de estado ou conteúdo.
3.11.3.4. Quando um novo consentimento é registrado.
3.11.3.5. Quando um consentimento existente é modificado.
3.11.4. Quando ocorrer algum evento o sistema deve enviar para a URL destino as informações suficientes para que seja possível capturar os dados do evento registrado.
3.11.5. O conector com URL destino deve suportar diferentes formas de autenticação como senha.

3.12. Gestão de Incidentes

3.12.1. A plataforma deve permitir a criação manual de incidentes.
3.12.2. Deve ser possível configurar os diferentes tipos de incidentes.
3.12.3. O sistema deve permitir definir responsáveis por um incidente.
3.12.4. A plataforma deve vincular diagnósticos do módulo de diagnósticos com um incidente de modo a mitigar incidentes de fornecedores e seu nível de maturidade.
3.12.5. O sistema deve exibir uma linha do tempo com todos os eventos e mudanças de um incidente.
3.12.6. Deve ser possível cadastrar vários impactos à privacidade do titular causado por um incidente.
3.12.7. O sistema deve permitir relacionar usuários, ativos e empresas com um determinado incidente.
3.12.8. Deve ser possível modificar os dados e o status de um determinado incidente.

3.12.9. Deve ser possível vincular riscos com um determinado incidente.
3.12.10. Deve ser possível anexar documentos e políticas em um determinado incidente.
3.12.11. A plataforma deve exibir um relatório de incidentes com no mínimo os critérios abaixo:
3.12.11.1. Linha do tempo de incidentes no período.
3.12.11.2. Incidentes por tipo de incidente.
3.12.11.3. Incidente pelo seu estágio de andamento.
3.12.11.4. Incidente por fornecedores.
3.12.11.5. Incidente por fonte/origem.
3.12.11.6. Incidente por nível do risco.
3.12.12. Deve ser possível vincular tarefas relacionadas a um incidente de modo que outras pessoas do time possam trabalhar na mitigação.

3.13. Data Discovery (descoberta de dados)

3.13.1. Deve possuir API para integração da plataforma com outros sistemas de modo que um sistema terceiro possa fazer buscas por dados pessoais e por tipos de dados pessoais encontrados
3.13.2. Deve permitir o monitoramento de, no mínimo, os seguintes ambientes:
3.13.2.1. Através de carregamento de Arquivos com as extensões: TXT, CSV, XML, PDF.
3.13.2.2. Oracle 12C e superiores.
3.13.2.3. MySQL.
3.13.2.4. Ambientes de FTP/FTPS.
3.13.2.5. Ambientes através de SSH (SFTP).
3.13.2.6. Sistema de arquivos (Storage/NFS).
3.13.2.7. Microsoft 365.
3.13.2.8. Google Drive.
3.13.2.9. Computadores de uma rede através do download de agentes.
3.13.3. Deve permitir o agendamento de execução do fluxo de descoberta de dados.
3.13.4. Deve permitir a customização de busca de dados pessoais a partir do uso de expressões regulares ou inteligência artificial.
3.13.5. Deve possuir controle de tipos de dados (categoria) e severidade de cada tipo.
3.13.6. Deve permitir percorrer todos os resultados da busca e saber onde estão os dados pessoais.
3.13.7. Deve permitir integração com o módulo de atendimento de pedidos para acelerar a automação do pedido.
3.13.8. O sistema deve possuir conexão nativa com o módulo de *data mapping* (mapeamento de dados) de modo que uma varredura já faça o trabalho inicial de mapeamento de dados com as operações de tratamento encontrados e seus dados pessoais.
3.13.9. O sistema deve permitir remover dados pessoais encontrados pelo sistema e colocar o dado em uma '*blacklist*' para não serem novamente indexados.
3.13.10. O sistema deve permitir limpar os resultados de uma varredura anterior quando for executar uma nova varredura.
3.13.11. O sistema deve ter componentes para Windows, Linux e Mac para que possa ser feita uma varredura de arquivos no computador em busca de dados pessoais armazenados.

3.14. Treinamento

3.14.1. O treinamento deverá ser focado no sistema como um todo e deverá abranger a capacitação de usuários com perfis de "utilizador" e "administrador".
3.14.1.1. Todos os módulos de treinamento deverão ser realizados no modelo EAD, a distância, com aulas remotas ao vivo.

3.14.2. O instrutor deverá estar certificado ou declarado apto pelo fabricante do sistema para ministrar o curso para o qual foi designado.
3.14.2.1. A CEDAE poderá, a qualquer momento, solicitar à contratada o fornecimento do currículo de qualquer instrutor, assim como a comprovação das informações fornecidas.
3.14.3. A segmentação funcional/turmas poderá ser ajustada entre a CONTRATANTE e CONTRATADA.
3.14.4. O treinamento deverá ser apoiado em manual técnico que deverá estar disponível na versão em arquivo PDF e antes das datas agendadas para os treinamentos.
3.14.5. O material de treinamento deverá estar atualizado conforme a versão do software disponibilizado.
3.14.6. Todo o processo de treinamento e os artefatos técnicos envolvidos deverão ser aprovados e homologados pela CEDAE.
3.14.7. O treinamento deverá ocorrer em ambiente de sistema e infraestrutura específico para esta finalidade.
3.14.8. O ambiente de treinamento deverá ser preparado pela CONTRATADA.
3.14.9. O treinamento será oficial pela fornecedora da solução.

3.14.10. Módulos de Treinamento

3.14.10.1. Módulo para Capacitação de Usuário Utilizador:
3.14.10.1.1. A Contratada deverá prever, no mínimo, 20 (vinte) horas para ministrar a capacitação, treinando 1 (uma) turmas com até 6 (seis) colaboradores.
3.14.10.1.2. O Módulo para Capacitação de Usuários Utilizador do sistema deverá proporcionar a capacitação de colaboradores da CEDAE na plena utilização das funcionalidades dos módulos de modo que possam ser futuros multiplicadores do conhecimento.

3.14.10.2. Módulo de Treinamento Técnico do Usuário Administrador:
3.14.10.2.1. A Contratada deverá prever, no mínimo, 30 (trinta) horas para ministrar a capacitação, treinando 1 (uma) turmas com até 5 (cinco) colaboradores.
3.14.10.2.2. O Módulo de Capacitação para Desenvolvedores na solução deverá proporcionar a capacitação de colaboradores da CEDAE nas rotinas de administração da ferramenta.

3.15. A proposta de preço deve conter as tabelas abaixo.

Licenças				
Item	Licenças	Quantidade	Valor Unitário R$	Valor Total R$
1	Usuário Utilizador	6		
2	Usuário administrador	5		
			Total R$	

Serviços Consumidos por Tarefa					
Item	Serviço	Unidade	Quantidade	Valor Unitário	Valor Total R$
1	Suporte e Update de Versão	mês	36		
2	Treinamento Utilizador	hora	20		
3	Treinamento Administrador	hora	30		
				Total R$	

3.16. ESPECIFICAÇÃO DO SERVIÇO

Item	Código IFS	ESPECIFICAÇÃO DO SERVIÇO	UNID	QUANT
		Indicar todos os requisitos desejados para o serviço a ser prestado, indicando se a contratação é de pessoa física ou jurídica, com descrições detalhadas das atividades, com precisão e clareza.		

3.17. SERVIÇO CONSUMIDOS POR TAREFA

3.17.1. Os Serviços Consumidos por Tarefa demandado pela CEDAE serão formalizados por meio de Ordens de Serviço (O.S);

3.17.1.1. As ordens de serviço deverão ser preenchidas da seguinte forma:

3.17.1.2. Data e hora da solicitação, descrição da solicitação, condição de aceite, prazo estimado de conclusão, nome do solicitante, aceite da ordem de serviço (assinatura do solicitante, após preenchimento por parte da contratada);

3.17.1.3. Data e hora da conclusão, detalhamento das ações executadas, condição de aceite atendida (S/N), responsável pela implementação, justificativa para condição de aceite não atendida.

3.17.1.4. Deverá ser criada uma O.S para cada demanda de Serviços Consumidos por Tarefa. As O.S deverão obedecer ao seguinte fluxo operacional:

3.17.1.5. A CEDAE emitirá O.S especificando o serviço solicitado;

3.17.1.6. A CONTRADATA executará e entregará os produtos e serviços especificados;

3.17.1.7. Não obstante as regras de recebimento do objeto estabelecidas no edital de licitação, a CEDAE realizará o aceite provisório e procederá à homologação dos produtos e serviços executados e entregues pela CONTRATADA;

3.17.1.8. A CEDAE, após a homologação, dará o aceite definitivo e liberação da O.S para faturamento;

3.17.1.9. O recebimento definitivo será realizado durante aceite definitivo, após recebimento provisório, caso não se constate nenhuma anormalidade no funcionamento e operacionalização do serviço realizado. O recebimento definitivo será feito pelos fiscais de contrato;

3.17.1.10. O recebimento definitivo deverá ser acompanhado de termo de aceite dos serviços. Sendo desatendida qualquer determinação do Termo de Referência, será solicitado à contratada que o serviço seja refeito, estabelecendo o prazo necessário para a sua execução/conclusão;

3.17.1.11. Só haverá o Recebimento Definitivo, após a análise da qualidade dos serviços prestados, resguardando-se a CEDAE o direito de não receber o objeto cuja qualidade seja comprovadamente baixa;

4. CRITÉRIO DE JULGAMENTO DA PROPOSTA

4.1. Menor preço global.

5. TIPO DE CONTRATAÇÃO E REGIME/FORMA DE EXECUÇÃO/FORNECIMENTO:

5.1. (X) SERVIÇO:

5.1.2. (x) de natureza contínua ou ( ) de escopo;

5.1.3. (___) com mão de obra alocada ou (X) sem mão de obra alocada;

5.1.4. (__) regime de execução por preço unitário; (X) Regime de execução por preço global; ou (___) Regime de execução por tarefa.

5.2. (___) AQUISIÇÃO:

5.2.1. (___) forma de fornecimento integral; (___) forma de fornecimento parcelada; ou ( ) forma de fornecimento contínua

6. PRAZO DE ENTREGA DO BEM OU DA PRESTAÇÃO DO SERVIÇO

6.1 Os serviços em epígrafe deverão ter início conforme ordem de início determinada pela CEDAE;
6.2 O Suporte Técnico e update de versão correspondente a 36 meses de serviço da mesma forma passará a vigorar a partir da data da Ordem de Início;
6.3 O prazo de vigência do Contrato será de 36 meses contados a partir do dia seguinte da autorização expressa expedida pela CEDAE (Ordem de Início), que será emitida após a publicação do extrato do instrumento contratual no Diário Oficial;
6.4 O prazo ora previsto poderá ser alterado por acordo entre as partes, por meio de termo aditivo, devendo ser observado, neste caso, os dispostos descritos no RILC;
6.5 A implantação da solução deverá ser concluída conforme cronograma físico/financeiro, após a publicação do contrato no DO-RJ;

7- LOCAL DE EXECUÇÃO OU ENTREGA DO BEM:

7.1 A prestação de serviços, quando presencial, deverão ocorrer no prédio sede da CEDAE, localizado na Av. Presidente Vargas, 2.655, Cidade Nova - Rio de janeiro - CEP 20.210-030

8- CONDIÇÕES DE RECEBIMENTO

8.1 As demandas solicitadas serão entregues conforme especificado nesse termo de referência.

9- PRAZO E CONDIÇÕES DE GARANTIA, MANUTENÇÃO E ASSISTÊNCIA TÉCNICA DO PRODUTO OU SERVIÇO

9.1 O prazo de vigência do Contrato será de 36 (trinta e seis) meses, podendo ter a sua duração prorrogada conforme o RILC (Regulamento Interno de Licitação e Contratos) e a lei Federal Nº 13.303, respeitado o prazo máximo de 60 (sessenta) meses.

10 - FORMA E CONDIÇÕES DE PAGAMENTO

10.1 Os pagamentos serão realizados na forma de prestações mensais e consecutivas, durante a vigência do contrato.

11- OBRIGAÇÕES DA CONTRATADA

11.1 Proibir a veiculação de publicidade ou qualquer outra informação acerca do objeto do contrato, salvo se houver prévia autorização da Administração da CEDAE;

11.2 Reparar, corrigir, remover e reconstruir, às suas expensas, no total ou em parte, os serviços efetuados referentes ao objeto em que se verifiquem vícios, defeitos ou incorreções resultantes da execução, conforme estabelecido neste Termo de Referência;

11.3 Comunicar por escrito qualquer anormalidade, prestando à CEDAE os esclarecimentos julgados necessários;

11.4 Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, por ocasião da execução do objeto licitado.

11.5 A CEDAE não aceitará, sob nenhum pretexto, a transferência de responsabilidade da CONTRATADA para outras entidades, sejam fabricantes, técnicos ou quaisquer outros;

11.6 Comunicar à CEDAE, por escrito, no prazo máximo de 05 (cinco) dias úteis que antecedem o prazo de vencimento das entregas, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos;

11.7 Comunicar imediatamente à CEDAE, a eventual alteração no endereço de sua sede, telefone, e-mail;

11.8 A CONTRATADA deverá se comprometer a manter todas as condições que garantam o sigilo das informações em custódia da CEDAE, bem como zelar pelos princípios que regem a Segurança da Informação: a Confidencialidade, Integridade e Disponibilidade; sendo responsável por qualquer evento

que viole algum destes princípios ou condições decorrentes da prestação de seus serviços, salvo em caso de quebra de sigilo determinada por autoridade judiciária;

11.9 A CONTRATADA será responsável civil, criminal e administrativamente por quaisquer danos causados pela prestação de seus serviços aos ativos da CEDAE, desde que a mesma seja responsável pelo fato causador do dano;

11.10 CONTRATADA deverá informar à CEDAE os incidentes de segurança que possam comprometer a confidencialidade, integridade ou disponibilidade do serviço prestado;

11.11 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todos os assuntos de interesse da CEDAE, que tomar conhecimento em razão da execução do objeto do Contrato, devendo orientar seus empregados nesse sentido.

12- AMOSTRA

12.1 Não se aplica.

13- VISITA TÉCNICA

13.1 Não se aplica.

14- ACORDO DE NÍVEIS DE SERVIÇO

14.1 As paradas para manutenção do sistema devem ser avisadas com antecedência de 48h e devem ser realizadas entre 23h e 6h, assegurando-se a prestação do serviço.

14.2 A eventual indisponibilidade do sistema para o recebimento de solicitações poderá gerar à CONTRATADA o desconto na fatura no montante de 0,5% (cinco décimos por cento) do valor mensal, por hora indisponível após o período máximo tolerado de paralisação de 1 (uma) hora seguida, limitadas ao somatório máximo mensal de 10 (dez) horas.

14.3 A reincidência sujeitará a CONTRATADA às penalidades previstas no contrato.

15- FORMALIZAÇÃO DO CONTRATO

15.1 É necessário, devido à natureza da prestação de serviço, a formalização do contrato.

16- CONDIÇÕES GERAIS

16.1 Não se aplica.

17- ASSINATURAS