1. APRESENTAÇÃO

Este manual integra o Programa de Governança em Privacidade e Proteção de Dados da **Fundação Carlos Alberto Vanzolini (FCAV)** e deve ser aplicado em conjunto com as políticas, as normas e os procedimentos internos correlatos. Seu objetivo é garantir a conformidade com a **Lei nº 13.709/2018** (Lei Geral de Proteção de Dados Pessoais – LGPD) e assegurar que, desde a concepção até o encerramento de cada projeto ou iniciativa, sejam adotadas medidas adequadas de proteção, classificação e tratamento de dados pessoais.

A adoção das diretrizes aqui estabelecidas é obrigatória para todas as áreas, gestores e equipes da FCAV, em todos os projetos e processos que envolvam o tratamento de dados pessoais, inclusive aqueles conduzidos por terceiros, parceiros ou contratados. As ações são orientadas pela Área de Privacidade e Proteção de Dados, que deve ser acionada sempre que for identificado novo projeto, processo ou atividade que envolva o tratamento de dados pessoais ou qualquer alteração relevante naqueles já existentes.

2. PRINCÍPIOS GERAIS

As atividades de tratamento de dados pessoais devem observar a boa-fé e os princípios previstos no artigo 6º da LGPD, bem como aqueles definidos na Política de Governança de Dados Pessoais da FCAV, resumidos na tabela a seguir.

PRINCÍPIO	DESCRIÇÃO	APLICAÇÃO PRÁTICA
Finalidade	Garantia de que o tratamento ocorra apenas para propósitos legítimos, específicos e informados ao titular.	Definir claramente, durante o planejamento do projeto, a finalidade do tratamento e, quando aplicável, descrevê-la no termo de consentimento ou na documentação de coleta de dados.
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular.	Garantir que a utilização dos dados seja coerente com os propósitos informados no momento de sua coleta ou entrada.
Necessidade	Limitação do tratamento ao mínimo necessário para atingir a finalidade.	Coletar apenas os dados estritamente necessários para a execução do projeto, evitando excessos.

Livre acesso	Garantia de que o titular possa consultar seus dados de forma facilitada.	Prever mecanismos que permitam identificar e atender solicitações de acesso e atualização, conforme o "Procedimento para atendimento às requisições do titular".
Qualidade dos dados	Garantia de exatidão, clareza e atualização dos dados tratados.	Validar a origem dos dados, atualizar informações sempre que necessário e evitar duplicidades.
Transparência	Garantia de informações claras, precisas e acessíveis aos titulares.	Assegurar que todos os documentos e comunicações com o titular quanto ao uso de seus dados utilizem linguagem clara e objetiva.
Segurança	Adoção de medidas técnicas e administrativas aptas a proteger os dados.	Cumprir a Política de Governança de Dados Pessoais e as normas de segurança da informação da FCAV, com apoio da Área de Tecnologia da Informação, adotando controles proporcionais ao tipo e à sensibilidade dos dados tratados.
Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento.	Avaliar riscos à privacidade durante a fase de planejamento e aplicar o "Procedimento de avaliação de *privacy by design*".
Não discriminação	Proibição de tratamento para fins discriminatórios ilícitos ou abusivos.	Evitar critérios de seleção, análise ou segmentação que possam gerar discriminação injustificada.
Responsabilização e prestação de contas	Demonstração da adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados.	Registrar evidências de conformidade em relatórios e formulários e no RoPA.* Revisar periodicamente as medidas adotadas.

*** RoPA: Registro das Atividades de Tratamento de Dados Pessoais (sigla do nome em inglês *Record of Processing Activities*).**

3. CLASSIFICAÇÃO DA INFORMAÇÃO

A proteção das informações tratadas nos projetos da FCAV é fundamental para garantir sua **confidencialidade, integridade e disponibilidade**, conforme previsto na Política de Segurança da Informação e nas normas internas relacionadas à gestão de incidentes, e o primeiro passo para proteger uma informação é classificá-la.

As informações devem ser classificadas pelo gestor do projeto ainda na **fase de planejamento**, com apoio da Área de Privacidade e Proteção de Dados e da Área de Tecnologia da Informação (TI), sempre que houver tratamento de dados pessoais ou de informações sensíveis, de acordo com as categorias adotadas na FCAV, apresentadas na tabela a seguir.

CLASSIFICAÇÃO	DESCRIÇÃO	EXEMPLOS
Confidencial	Informação de acesso restrito a pessoas autorizadas e cuja divulgação indevida possa causar impacto significativo à instituição, aos parceiros ou aos titulares de dados pessoais.	➔ Dados pessoais sensíveis. ➔ Informações estratégicas. ➔ Registros financeiros. ➔ Documentos contratuais.
Restrita	Informação interna que não deve ser divulgada externamente sem prévia autorização.	➔ Dados operacionais de projeto. ➔ Listas de contatos institucionais. ➔ Relatórios internos.
Interna	Informação destinada a uso interno da FCAV, sem necessidade de confidencialidade elevada.	➔ Comunicados internos. ➔ Cronogramas. ➔ Documentos administrativos sem dados pessoais.
Pública	Informação destinada à ampla divulgação, sem restrição de acesso.	➔ Materiais de comunicação. ➔ Resultados públicos de projetos. ➔ Relatórios institucionais.

Registro da classificação

A classificação dos dados pessoais e das informações sensíveis tratadas, bem como a forma de proteção aplicada, deve ser registrada pela área responsável no "Formulário de avaliação de tratamento de dados pessoais", como evidência do projeto.

A Área de Privacidade e Proteção de Dados analisa as informações preenchidas nesse formulário, indica medidas adicionais necessárias e, quando aplicável, atualiza o RoPA. Dessa forma, os gestores não preenchem o RoPA, eles devem informar corretamente, no "Formulário de avaliação de tratamento de dados pessoais", o tratamento de dados pessoais e informações sensíveis sob sua responsabilidade, o que permite à Área de Privacidade e Proteção de Dados fazer inserções e alterações no RoPA, se pertinente.

Incidentes com informação confidencial ou restrita

Qualquer incidente de segurança ou suspeita de vazamento que envolva informação classificada como confidencial ou restrita deve ser comunicado imediatamente à Área de Privacidade e Proteção de Dados e à Área de TI, conforme definido na "Norma de gestão de incidentes de segurança da informação" e na "Norma de gestão de incidentes de violação de dados pessoais".

4. REGISTRO DAS ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS

O Registro das Atividades de Tratamento de Dados Pessoais (RoPA) é um documento mantido exclusivamente pela Área de Privacidade e Proteção de Dados, conforme exigido pela LGPD. Nenhuma outra área ou gestor atualiza o RoPA diretamente.

Sempre que uma área identificar novo processo, novo projeto ou nova atividade que envolva o tratamento de dados pessoais, novo fluxo de envio ou recebimento de dados pessoais ou, ainda, alteração em tratamento já existente, seu gestor deve preencher o "Formulário de avaliação de tratamento de dados pessoais", como etapa inicial obrigatória para avaliação e definição dos próximos passos. Esse formulário solicita apenas as informações de negócio necessárias para que a Área de Privacidade e Proteção de Dados faça a análise técnica, na qual ela:

- Avalia o tratamento de dados pessoais e informações sensíveis e verifica sua conformidade com a LGPD;
- Define a base legal, os riscos, os pontos de atenção e as medidas obrigatórias para o tratamento em questão;
- Indica medidas adicionais (por exemplo, cláusulas contratuais, ajustes no fluxo de dados, anonimização de dados pessoais, apoio da Área de TI ou da Área de Contratos etc.);
- Atualiza o RoPA, inserindo novo registro ou alterando registro preexistente que corresponda ao tratamento em questão;
- Encaminha orientações formais à área responsável pelo tratamento.

O RoPA é utilizado pela FCAV para:

documentar todos os tratamentos de dados pessoais realizados pelas áreas;

- Subsidiar avaliações de risco e ações de mitigação;
- Apoiar auditorias, análises internas e exigências regulatórias;
- Demonstrar conformidade aos titulares dos dados pessoais e às autoridades competentes.

5. DIRETRIZES PARA PROJETOS

As diretrizes a seguir devem ser observadas desde a fase de concepção e planejamento de qualquer projeto, processo ou atividade que envolva o tratamento de dados pessoais, tanto em iniciativas executadas diretamente pela FCAV quanto em parcerias com terceiros. Elas são parte integrante das etapas de aprovação, execução e encerramento de projetos na FCAV.

5.1 ACIONAMENTO INICIAL VIA FORMULÁRIO (OBRIGATÓRIO)

O **gestor** responsável pelo projeto deve preencher o "Formulário de avaliação de tratamento de dados pessoais" sempre que sua área identificar:

- Novo projeto, processo ou atividade que envolva tratamento de dados pessoais;
- Novo fluxo de envio ou recebimento de dados pessoais;
- Uso de nova ferramenta ou sistema que trate dados pessoais;
- Alteração relevante em tratamentos de dados pessoais preexistentes.

Nesse formulário, devem ser informados:

- Área responsável;
- Departamento, se houver;
- Nome do processo/atividade;
- Motivo do processo/atividade (por que existe);
- Dados pessoais envolvidos no processo/atividade (que tipo de dado passa pelo processo/atividade);
- Compartilhamento com outras áreas **internas**, se houver;
- Compartilhamento com instituições, empresas ou pessoas **externas** à FCAV, se houver;
- Sistemas e plataformas utilizados;
- Local em que os dados pessoais ficam armazenados (onde são salvos);
- Como os dados pessoais chegam à área/processo/atividade;
- Responsável pelo preenchimento do formulário;
- *E-mail* do responsável pelo preenchimento;
- Eventuais documentos necessários à análise (opcional; se houver, devem ser anexados);
- Comentários pertinentes.

Com base nas informações preenchidas no formulário, a **Área de Privacidade e Proteção de Dados** avalia o tratamento e verifica sua conformidade com a LGPD, identifica riscos, fragilidades e medidas obrigatórias, indica medidas adicionais (como apoio da Área de TI ou da Área de Contratos, entre outras), atualiza o RoPA e encaminha orientações formais para implementação do projeto.

5.2 PLANEJAMENTO E DOCUMENTAÇÃO DO PROJETO

Durante o planejamento, o **gestor** deve:

- Avaliar se o uso de dados pessoais é necessário e proporcional à finalidade;
- Identificar se haverá compartilhamento de dados pessoais com terceiros;
- Indicar no "Formulário de avaliação de tratamento de dados pessoais" quais tipos de tratamento de dados pessoais serão realizados e se haverá compartilhamento;
- Definir local de guarda e tipo de controle de acesso aos documentos do projeto;
- garantir que apenas pessoas autorizadas tenham acesso às informações.

A análise técnica do tratamento de dados pessoais (base legal, riscos, medidas de segurança, necessidade de cláusulas contratuais e controles) é realizada pela Área de Privacidade e Proteção de Dados.

5.3 COLETA E TRATAMENTO DE DADOS PESSOAIS

Quando o projeto envolver **coleta direta de dados pessoais**, deve-se:

- Informar claramente aos titulares dos dados a finalidade do tratamento;
- Utilizar *checkbox* obrigatório ou termo eletrônico de ciência, quando necessário;
- Evitar coleta excessiva de dados, aplicando o princípio da necessidade;
- Garantir segurança e sigilo dos dados durante todo o ciclo de vida do projeto;
- Seguir as orientações emitidas pela Área de Privacidade e Proteção de Dados após análise do "Formulário de avaliação de tratamento de dados pessoais".

5.4 RELAÇÃO COM TERCEIROS E FORNECEDORES

Quando o projeto envolver terceiros, prestadores de serviços ou parceiros que tenham acesso a dados pessoais, o **gestor** deve indicar esse compartilhamento no "Formulário de avaliação de tratamento de dados pessoais".

Após receber o formulário preenchido, a **Área de Privacidade e Proteção de Dados** faz a análise técnica e:

- Verifica se o terceiro realmente terá acesso a dados pessoais;

- Solicita que o terceiro seja submetido ao “Questionário de proteção de dados”, se pertinente;
- Avalia o nível de conformidade e os riscos associados ao terceiro;
- Indica as medidas a serem adotadas, inclusive cláusulas contratuais obrigatórias, controles adicionais de segurança e restrições ao compartilhamento.

Quando acionada, a **Área de Contratos** deve incluir ou ajustar cláusulas contratuais obrigatórias conforme orientações da Área de Privacidade e Proteção de Dados, a fim de assegurar:

- confidencialidade e sigilo dos dados pessoais compartilhados;
- adoção de medidas de segurança compatíveis;
- proibição de uso indevido dos dados pessoais compartilhados;
- devolução ou descarte seguro dos dados pessoais ao término do contrato.

O compartilhamento externo **não deve ocorrer** antes da conclusão dessas medidas, ou seja, um terceiro se torna apto a receber dados pessoais que estejam sob responsabilidade da FCAV somente após a avaliação do “Questionário de proteção de dados” e a validação da Área de Privacidade e Proteção de Dados.

6. GESTÃO OPERACIONAL DE DADOS DURANTE A EXECUÇÃO DOS PROJETOS

A gestão dos dados durante a execução dos projetos deve observar as diretrizes de privacidade, segurança da informação e governança previstas na LGPD e nas políticas internas da FCAV. Para garantir rastreabilidade, transparência e responsabilização (*accountability*) em todas as fases dos projetos (planejamento, execução, monitoramento e encerramento), as áreas da FCAV têm responsabilidades específicas, conforme apresentado a seguir.

6.1 MATRIZ DE RESPONSABILIDADES

A matriz RACI é um registro das áreas ou pessoas que atuam como responsáveis, aprovadores, consultados e informados em processos e/ou atividades:

- R – Responsável: é quem executa a atividade na prática, assume a execução da tarefa e a entrega da etapa;
- A – Aprovador (responsável final): é quem valida, aprova ou responde pela atividade, garante que o resultado esteja correto e em conformidade;
- C – Consultado: é quem deve ser consultado para fornecer apoio técnico, orientação ou parecer especializado durante a execução da tarefa;
- I – Informado: é quem deve ser informado sobre o andamento ou o resultado da tarefa, mas não executa, não aprova e não precisa ser consultado.

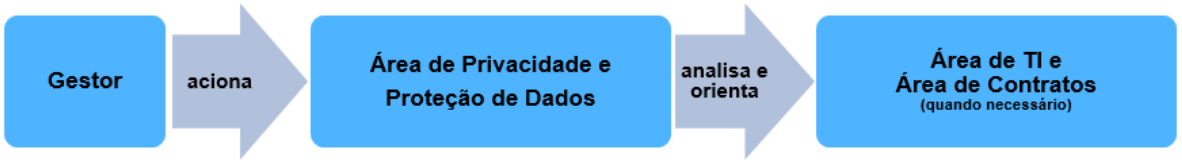
A matriz apresentada a seguir deve ser usada por todas as áreas da FCAV como referência; ela indica quem é responsável, quem aprova, quem apoia tecnicamente e quem apenas acompanha atividades do tratamento de dados pessoais.

ATIVIDADE	GESTOR RESPONSÁVEL	ÁREA DE PRIVACIDADE E PROTEÇÃO DE DADOS	ÁREA DE TI	ÁREA DE CONTRATOS
Identificar se há envio ou recebimento de dados pessoais	R	I	I	I
Preencher o "Formulário de avaliação de tratamento de dados pessoais"	R	C	I	I
Analisar se há tratamento de dados pessoais	I	A/R	C	C
Definir base legal, riscos e medidas obrigatórias	I	A/R	C	C
Indicar ajustes no fluxo, medidas técnicas ou processuais	I	A/R	C	I
Acionar a Área de TI quando forem necessárias medidas de segurança ou ferramentas	I	A/R	C	I
Acionar a Área de Contratos quando forem necessárias cláusulas ou alterações contratuais	I	A/R	I	C
Avaliar terceiros ("Questionário de proteção de dados")	I	A/R	I	C

Coletar adequadamente o consentimento do titular de dados pessoais (quando aplicável)	R	A	C	I
Implementar medidas técnicas de segurança	I	C	A/R	I
Comunicar incidentes ou suspeitas	R	A	C	I
Armazenar e proteger documentos	R	C	C	I
Revisar acessos ao longo do projeto	R	C	C	I
Atualizar orientações e requisitos de privacidade	I	A/R	C	I
Monitorar e revisar boas práticas	C	A/R	C	I

6.2 DISPOSIÇÕES COMPLEMENTARES

As responsabilidades operacionais durante a execução de projetos e processos devem seguir a lógica do **fluxo institucional de privacidade** da FCAV:



Durante a execução de atividades que envolvam o tratamento de dados pessoais, cada área deve atuar conforme seu papel nesse fluxo, garantindo segurança, rastreabilidade e conformidade com a LGPD.

O gestor responsável pelo processo/projeto é quem percebe, no dia a dia, quando há envio, recebimento ou uso de dados pessoais. Sempre que isso ocorrer, ele deve preencher o "Formulário de avaliação de tratamento de dados pessoais" e acionar a Área de Privacidade e Proteção de Dados. Cabe ao gestor seguir integralmente as orientações emitidas pela Área de Privacidade e Proteção de Dados, inclusive diretrizes sobre consentimento de titular de dados, controle de acessos, guarda de documentos, avaliação de terceiros e ajustes no fluxo de dados. Também é sua responsabilidade comunicar imediatamente qualquer incidente, suspeita ou risco que envolva dados pessoais.

A Área de Privacidade e Proteção de Dados conduz toda a análise técnica: confirma se existe tratamento de dados pessoais, avalia riscos, define base legal, estabelece medidas obrigatórias e identifica controles mínimos. Ela também avalia terceiros por meio do "Questionário de proteção de dados", aciona a Área de TI e/ou a Área de Contratos, quando necessário, e mantém o RoPA atualizado com base nas informações fornecidas pelas áreas e pelos gestores.

A Área de TI atua quando as medidas exigidas envolvem tecnologia, segurança ou sistemas. Isso inclui implementação de controles, ativação de *logs* e rastreabilidade, apoio em pseudonimização ou anonimização de dados pessoais, bloqueio e exclusão definitiva de acessos conforme as normas de segurança da informação da FCAV.

A Área de Contratos é acionada sempre que há necessidade de cláusulas contratuais obrigatórias relacionadas à proteção, à confidencialidade e/ou ao descarte seguro de dados pessoais. Sua atuação ocorre sob orientação da Área de Privacidade e Proteção de Dados.

6.3 CONTROLE DE ACESSO E GUARDA DE DOCUMENTOS

Os repositórios eletrônicos utilizados em projetos e processos que envolvam tratamento de dados pessoais devem possuir acesso controlado e rastreável, restrito apenas às pessoas formalmente autorizadas.

O gestor responsável pelo processo/projeto atua como guardião do repositório; ele deve:

- solicitar inclusão e exclusão de acessos conforme a evolução da equipe;
- revisar periodicamente (no mínimo a cada trimestre) a lista de acessos ativos;
- garantir que documentos que contenham dados pessoais ou sensíveis estejam armazenados em pastas com controle de acesso restrito;
- solicitar à Área de TI o bloqueio imediato de acessos em caso de desligamento, troca de função ou término de contrato;
- garantir, ao encerrar o processo/projeto, a execução de revisão final de acessos e exclusão segura de documentos não essenciais.

A Área de TI é responsável por:

- implementar controles de autenticação e auditoria (*logs*) que possibilitem rastreabilidade em caso de incidente;
- disponibilizar estruturas de pastas e sistemas que permitam controle adequado de acesso;
- apoiar a aplicação de pseudonimização ou uso de dados agregados/anonimizados, quando indicado pela Área de Privacidade e Proteção de Dados;
- assegurar que as exclusões sejam realizadas de forma segura e definitiva, conforme as normas de segurança e privacidade da FCAV.

A Área de Privacidade e Proteção de Dados deve acompanhar a aplicação das práticas e medidas pertinentes pela Área de TI e pelo gestor/área responsável, orientando-os sobre regras de retenção, descarte seguro e acesso adequado a documentos

7. DIRETRIZES PARA ENCERRAMENTO DE PROJETOS

O encerramento de projetos ou processos que envolvam o tratamento de dados pessoais deve garantir a segurança, a integridade e a eliminação adequada das informações usadas durante a execução do projeto, prevenindo qualquer uso indevido após o término das atividades. Para isso, devem ser executadas as ações descritas na tabela a seguir.

ETAPA DO ENCERRAMENTO		DESCRIÇÃO DA AÇÃO
1	**Revisão e revogação de acessos**	Revisar e remover todos os acessos de usuários que não devam mais ter contato com os dados ou documentos do projeto, mediante solicitação à Área de TI de bloqueio imediato de acessos remanescentes.

2	**Verificação de cópias indevidas de dados**	Confirmar que não existem cópias de dados pessoais ou sensíveis em dispositivos pessoais, *e-mails*, mídias externas ou pastas não autorizadas.
3	**Centralização final da documentação**	Reunir toda a documentação final em repositório seguro (ferramenta institucional), com acesso restrito ao gestor responsável e à equipe autorizada.
4	**Entrega de dados ao cliente (quando aplicável)**	Transferir ao cliente apenas os dados necessários, mediante termo de ciência e responsabilidade, informando a eliminação segura dos demais registros.
5	**Descarte seguro ou anonimização de dados pessoais**	Aplicar descarte seguro ou anonimização dos dados pessoais cujo uso ou finalidade tenha se encerrado, conforme as diretrizes do Programa de Governança em Privacidade e demais normas internas da FCAV.
6	**Registro das ações de encerramento**	Registrar as ações realizadas (revisão de acessos, descarte, entrega ao cliente etc.) na documentação do projeto. A Área de Privacidade e Proteção de Dados atualizará o RoPA, quando aplicável.

8. COMPARTILHAMENTO DE DADOS PESSOAIS

O compartilhamento de dados pessoais em projetos e processos da FCAV pode ser feito com:

- áreas internas, para execução das atividades;
- prestadores de serviços e parceiros contratados, após avaliação de conformidade e validação contratual;
- áreas do cliente, quando necessário ao objeto contratado e conforme orientações da Área de Privacidade e Proteção de Dados.

O compartilhamento pode ocorrer somente quando necessário e deve ser previamente informado no "Formulário de avaliação de tratamento de dados pessoais", para que a Área de Privacidade e Proteção de Dados avalie:

- se o compartilhamento é adequado e proporcional;
- se há base legal aplicável;
- se devem ser adotadas medidas adicionais;
- se o terceiro precisa ser avaliado por meio do "Questionário de proteção de dados";
- se são necessárias cláusulas contratuais específicas.

O compartilhamento deve ocorrer exclusivamente por canais corporativos oficiais e seguros, em conformidade com a Política de Segurança da Informação da FCAV. É vedado o uso de *e-mails* pessoais, aplicativos de mensagens instantâneas (como WhatsApp) e qualquer canal informal para envio, recebimento ou armazenamento de informações que contenham dados pessoais ou confidenciais.

Sempre que houver necessidade de compartilhamento, deve-se:

- utilizar apenas canais e sistemas corporativos autorizados (Google Chat, Google Drive corporativo e *e-mail* institucional);
- garantir que o destinatário esteja formalmente autorizado e ciente de suas responsabilidades;
- adotar medidas técnicas de segurança apropriadas, como controle de acesso e criptografia;
- formalizar o compartilhamento por meio de contrato com cláusulas específicas de proteção de dados ou termo de confidencialidade, quando aplicável.

O QUE FAZER ✅	O QUE NÃO FAZER ❌
Usar somente canais corporativos (Google Chat, Google Drive corporativo e *e-mail* institucional).	Utilizar WhatsApp, *e-mail* pessoal, Google Drive pessoal, USB ou qualquer canal informal.
Informar o compartilhamento no "Formulário de avaliação de tratamento de dados pessoais".	Compartilhar dados sem comunicar a Área de Privacidade e Proteção de Dados.
Aguardar a análise e a orientação da Área de Privacidade e Proteção de Dados antes de qualquer envio externo.	Enviar dados a cliente, fornecedor ou parceiro sem prévia avaliação/validação.
Solicitar avaliação do terceiro via "Questionário de proteção de dados" (quando indicado pela Área de Privacidade e Proteção de Dados).	Conceder acesso a terceiros não avaliados ou sem cláusulas contratuais adequadas.
Garantir que o destinatário esteja formalmente autorizado e ciente de suas responsabilidades.	Enviar dados a pessoas externas "para facilitar", "para agilizar" ou "porque sempre fizemos assim".
Adotar medidas técnicas de segurança (controle de acesso e criptografia, quando aplicável).	Manter arquivos sensíveis sem proteção, expostos ou com acesso irrestrito.
Formalizar o compartilhamento com cláusulas contratuais de proteção de dados ou termo de confidencialidade.	Compartilhar dados apenas com base em acordos verbais, confiança ou relações informais.

Garantir que o compartilhamento tenha base legal e esteja de acordo com as orientações da Área de Privacidade e Proteção de Dados.	Compartilhar dados “porque o cliente pediu” ou “porque o fornecedor precisa deles”.
Tomar as medidas necessárias para que a Área de Privacidade e Proteção de Dados registre o compartilhamento no RoPA.	Registrar o compartilhamento diretamente no RoPA ou tentar atualizar controles sem orientação.

9. RESPONSABILIDADES

A conformidade com a LGPD é uma responsabilidade compartilhada entre todas as áreas da FCAV. Todas as partes devem atuar de forma integrada para garantir a aplicação das diretrizes deste manual, a segurança das informações e o cumprimento das normas internas de privacidade. As responsabilidades são distribuídas como apresentado a seguir.

9.1 GESTORES RESPONSÁVEIS POR PROCESSO OU PROJETO

- Acionar a Área de Privacidade e Proteção de Dados sempre que houver envio, recebimento ou uso de dados pessoais, fornecendo-lhe as informações de negócio necessárias por meio do "Formulário de avaliação de tratamento de dados pessoais".
- Seguir integralmente as orientações emitidas pela Área de Privacidade e Proteção de Dados.
- Garantir o controle adequado de acessos e a proteção dos documentos durante a execução do processo/projeto.
- Solicitar bloqueio de acessos quando integrantes deixarem de atuar no processo/projeto.
- Comunicar imediatamente qualquer incidente, risco ou suspeita que envolva dados pessoais.
- Realizar as ações de encerramento previstas (revisão de acessos, descarte seguro, entrega ao cliente etc.).

9.2 EQUIPES DAS ÁREAS RESPONSÁVEIS POR PROCESSO OU PROJETO

- Tratar apenas os dados pessoais estritamente necessários para a atividade.
- Utilizar exclusivamente canais corporativos autorizados.
- Proteger documentos e informações sob sua responsabilidade.
- Comunicar incidentes ou riscos ao gestor responsável e à Área de Privacidade e Proteção de Dados.

9.3 ÁREA DE PRIVACIDADE E PROTEÇÃO DE DADOS

- Conduzir a análise técnica de todos os tratamentos informados via "Formulário de avaliação de tratamento de dados pessoais".
- Definir base legal, riscos, medidas obrigatórias e controles mínimos.
- Avaliar terceiros por meio do "Questionário de proteção de dados".
- Orientar as áreas sobre consentimento, retenção, descarte, segurança e ajustes necessários.
- Acionar a Área de TI e a Área de Contratos, quando necessário.
- Manter o RoPA atualizado com base nas informações fornecidas pelas áreas.
- Apoiar na gestão de incidentes de segurança e no atendimento a titulares de dados pessoais.

9.4 ÁREA DE TECNOLOGIA DA INFORMAÇÃO

- Implementar e monitorar medidas técnicas de segurança (*logs*, rastreabilidade, autenticação).
- Incluir, alterar e bloquear acessos conforme solicitações dos gestores.
- Apoiar na pseudonimização e na anonimização de dados pessoais e no controle de guarda e descarte seguro.
- Realizar exclusões definitivas de acessos conforme as normas internas da FCAV.

9.5 ÁREA DE CONTRATOS

- Incluir e validar cláusulas obrigatórias de proteção, confidencialidade e descarte seguro de dados em contratos com terceiros e parceiros.
- Atuar conforme orientações da Área de Privacidade e Proteção de Dados quanto às medidas contratuais necessárias.

9.6 COLABORADORES E PARCEIROS

- Agir com responsabilidade no tratamento de dados pessoais.
- Utilizar apenas canais e ferramentas institucionais para tratamento de dados pessoais.
- Cumprir as políticas, as normas e as orientações da FCAV relacionadas à LGPD.

10. DÚVIDAS, APOIO E CONSCIENTIZAÇÃO

A proteção de dados pessoais é um compromisso contínuo da FCAV e depende da atuação responsável de todas as áreas e pessoas envolvidas.

A Área de Privacidade e Proteção de Dados está disponível para apoiar na interpretação deste manual, orientar a aplicação das diretrizes nele estabelecidas, esclarecer dúvidas sobre tratamentos de dados específicos, avaliar riscos, conduzir análises de terceiros e contribuir com ações de conscientização e treinamento.

Sempre que houver dúvidas sobre a aplicação da LGPD em projetos e processos, necessidade de apoio na avaliação de novos tratamentos ou suspeita de incidente que envolva dados pessoais, o canal oficial para comunicação com a Área de Privacidade e Proteção de Dados é o *e-mail* suportelgpd@vanzolini.org.br.

Esse contato é incentivado sempre que houver incerteza: perguntar é parte fundamental da cultura de proteção de dados da FCAV.

11. NATUREZA DE ALTERAÇÕES

Revisão	Alterações	Data
00	Emissão Inicial	09/02/2026