



Diretrizes Internas de Recolha Ética e Governança de Dados

Internal Guidelines for Ethical Data Collection and Data Governance

*Guia operacional para equipas de campo e dados • Declaração de diligência para
clientes e parceiros*

Controlo do documento | Document control

Título Title	Diretrizes Internas de Recolha Ética e Governança de Dados Internal Guidelines for Ethical Data Collection and Data Governance
Proprietário Owner	Data Governance & Research Ethics
Patrocinador Sponsor	Data4Moz Executive Management
Versão Version	1.0
Estado Status	Approved
Aprovado por Approved by	Antonio Inguane
Assinatura Signature	
Data de aprovação Approval date	November 17 th , 2025
Próxima revisão Next review	November 2027, or earlier after a material legal, risk, platform or partner review.
Classificação Classification	Internal guidance • Shareable with clients and partners

Como utilizar | How to use

1. Português: use a Parte I e os anexos em português no planeamento, formação, campo, análise e encerramento.
2. English: use Part II and the English annexes for client assurance, contracting, training and oversight.
3. Apply the stricter rule where law, ethics approval, contract or donor terms exceed this baseline. Record the project-specific decision in the Data Responsibility Plan.

LEGAL STATUS GATE | VALIDADE DO ESTATUTO JURÍDICO

The legal review is date-stamped 16 August 2026. The dedicated personal-data bill was still reported as pending, and Laws 13/2026 and 14/2026 were published with delayed commencement. Data4Moz must obtain a fresh Mozambican legal-status check before adoption and at every high-risk project gate.

Abreviatura | Acronyms

ABREVIATURA	DESIGNAÇÃO
AR	Assembleia da República
BI	Bilhete de Identidade
CICV	Comité Internacional da Cruz Vermelha
CNBS	Comité Nacional de Bioética para a Saúde
CSIRT	Equipa de Resposta a Incidentes de Segurança Informática
DPA	Acordo de Tratamento de Dados, do inglês Data Processing Agreement
GPS	Sistema de Posicionamento Global
HIV	Vírus da Imunodeficiência Humana
IA	Inteligência Artificial
IACM	Instituto de Aviação Civil de Moçambique
IASC	Comité Permanente Interagências
INE	Instituto Nacional de Estatística
INM	Imprensa Nacional de Moçambique
INS	Instituto Nacional de Saúde
INTIC	Instituto Nacional de Tecnologias de Informação e Comunicação
M&A	Monitoria e Avaliação
MFA	Autenticação Multifactor
OCHA	Escritório das Nações Unidas para a Coordenação de Assuntos Humanitários
ODK	Open Data Kit, conjunto aberto de ferramentas para recolha de dados
OMS	Organização Mundial da Saúde
PIN	Número de Identificação Pessoal
QA	Garantia da Qualidade
RGPD	Regulamento Geral sobre a Protecção de Dados
RPAS	Sistema de Aeronave Pilotada Remotamente
SFTP	Protocolo de Transferência de Ficheiros através de SSH
SMS	Serviço de Mensagens Curtas
UA	União Africana
UNEG	Grupo de Avaliação das Nações Unidas
UNICEF	Fundo das Nações Unidas para a Infância
VBG	Violência Baseada no Género
WIPO	Organização Mundial da Propriedade Intelectual, utilizada no nome WIPO Lex

Índice operacional | Operational contents

PORTUGUÊS	PÁG.	ENGLISH	PAGE
PARTE I. DIRETRIZES EM PORTUGUÊS	4	PART II. ENGLISH GUIDELINES	22
1. Estatuto, finalidade e utilização	4	1. Status, purpose and use	22
2. Âmbito, termos e classificação dos dados	4	2. Scope, terms and data classification	22
3. Princípios fundamentais	5	3. Core principles	23
4. Portão obrigatório antes do campo	6	4. Mandatory pre-field gate	24
5. Entrada comunitária e sensibilidade cultural em Moçambique	7	5. Community entry and cultural sensitivity in Mozambique	25
6. Seleção, contacto e qualidade no terreno	8	6. Selection, contact and field quality	26
7. Consentimento informado	9	7. Informed consent	26
8. Saúde, nutrição, VBG, protecção e outros temas de alto risco	10	8. Health, nutrition, GBV, protection and other high-risk topics	27
9. GPS, fotografia, áudio, vídeo, imagens e drones	11	9. GPS, photography, audio, video, imagery and drones	28
10. Procedimentos por meio de recolha	11	10. Collection-medium procedures	29
11. Utilização, partilha, retenção e eliminação	12	11. Use, sharing, retention and destruction	30
12. Anonimização e divulgação responsável	13	12. Anonymisation and responsible disclosure	31
13. Privacidade e segurança ao longo do ciclo de vida	14	13. Privacy and security throughout the lifecycle	31
14. Incidentes de dados e violações	14	14. Data incidents and breaches	31
15. Funções e responsabilidades	15	15. Roles and responsibilities	32
16. Formação, supervisão e conduta	15	16. Training, supervision and conduct	33
17. Reclamações, direitos e reparação	16	17. Complaints, rights and remedy	33
18. Quadro jurídico e normativo	16	18. Legal and standards framework	33
19. Monitoria, excepções e encerramento	17	19. Monitoring, exceptions and closure	34
ANEXOS OPERACIONAIS EM PORTUGUÊS	18	ENGLISH OPERATIONAL ANNEXES	35
Anexo A. Cartão de bolso do enumerador	19	Annex A. Enumerator pocket card	36
Anexo B. Guião-base de consentimento oral para adulto	19	Annex B. Adult oral-consent base script	36
Anexo C. Guião-base de assentimento para criança/adolescente	19	Annex C. Child/adolescent assent base script	36
Anexo D. Consentimento adicional para GPS, gravação e imagem	20	Annex D. Additional GPS, recording and image permission	37
Anexo E. Triagem de Avaliação de Impacto	20	Annex E. Impact-assessment screening	37
Anexo F. Lista de verificação para partilha	20	Annex F. Sharing checklist	37
Anexo G. Ficha de incidente	20	Annex G. Incident record	37
Anexo H. Verificação do supervisor	21	Annex H. Supervisor verification	37
Anexo I. Dossier de conformidade e encerramento	21	Annex I. Compliance and closure file	38
Anexo J. Fontes autorizadas e data de verificação	21	Annex J. Authoritative sources and verification date	38

PARTE I. DIRETRIZES EM PORTUGUÊS

1. Estatuto, finalidade e utilização

Estas Diretrizes Internas de Recolha Ética e Governação de Dados estabelecem os requisitos mínimos da Data4Moz para planear, recolher, transferir, tratar, analisar, partilhar, conservar e eliminar dados obtidos junto de pessoas, agregados familiares, comunidades, instituições e espaços geográficos. Aplicam-se a trabalhadores, consultores, subcontratados e parceiros que actuem em nome da Data4Moz.

O documento tem duas funções. É um manual operacional para equipas de campo e de dados e é uma declaração verificável dos compromissos que a Data4Moz assume perante participantes, clientes, autoridades e financiadores. Nenhum contrato, prazo ou pedido de cliente autoriza uma equipa a reduzir estas salvaguardas. Quando a lei, uma aprovação ética ou um contrato exigir uma medida mais rigorosa, prevalece a exigência mais rigorosa.

O NOSSO PRINCÍPIO: Nenhuma colecta e recolha de dados inicia sem protocolo aprovado, finalidade definida, instrumentos testados, responsabilidades contratuais esclarecidas, base legal confirmada, consentimento adequado e salvaguardas proporcionais ao risco.

1.1 Pressupostos usados nesta versão

4. Cobertura nacional, com trabalho em áreas urbanas, rurais, remotas, costeiras e afectadas por emergências ou conflito.
5. Recolha digital principalmente em KoboToolbox/ODK e ArcGIS Survey123/Field Maps, com formulários em papel quando necessário.
6. Dados socioeconómicos e de agregados familiares; saúde e nutrição; crianças e adolescentes; protecção e violência baseada no género (VBG); agricultura, meios de vida e recursos naturais; GPS, fotografia, áudio, vídeo, imagens e drones.
7. Clientes e financiadores variados. As obrigações específicas de cada doador são verificadas no contrato e anexadas ao Plano de Responsabilidade de Dados do Projecto.
8. A Data4Moz pode actuar como responsável pelo tratamento, processador por conta do cliente, ou ambos em fases diferentes. O contrato deve atribuir cada função antes de a configuração das plataformas.

1.2 Aprovação e revisão

O documento entra em vigor quando aprovado pela Direcção da Data4Moz. Deve ser revisto pelo menos anualmente e sempre que houver mudança legal relevante, novo tipo de dado, nova plataforma, incidente grave ou requisito do cliente ou parceiro. Os campos de aprovação, contactos de reclamação e responsáveis de segurança devem ser preenchidos antes da adopção formal.

NOTA LEGAL: Esta política traduz requisitos operacionais e fontes verificadas até 16 de Agosto de 2026. Não substitui parecer jurídico. Antes da aprovação e em cada projecto de alto risco, a Data4Moz deve obter confirmação de um jurista habilitado em Moçambique sobre diplomas vigentes, regulamentos, autorizações e obrigações sectoriais.

2. Âmbito, termos e classificação dos dados

2.1 O que está abrangido

As regras aplicam-se a entrevistas, grupos focais, observação, medições antropométricas, registos administrativos, listas de beneficiários, auditorias, monitoria e avaliação, censos comunitários, inquéritos, mapas participativos, rastreio de activos, telemetria, imagens de satélite ou drone, fotografias, gravações, dados recebidos de clientes e dados derivados por análise ou inteligência artificial.

Também abrangem metadados. Data, hora, identificador do dispositivo, trilho GPS, duração da entrevista, nome do enumerador e histórico de edições podem identificar uma pessoa ou revelar a localização e devem ser protegidos.

2.2 Definições operacionais

9. **Dados pessoais:** informação que identifica ou pode razoavelmente identificar uma pessoa, directa ou indirectamente.
10. **Dados sensíveis:** dados cuja divulgação ou uso indevido pode causar discriminação, estigma, violência, perda de benefícios, sanção, dano económico ou invasão grave da privacidade. Incluem saúde, deficiência, HIV, VBG, protecção, vida sexual, crianças, biometria, opiniões políticas, religião, filiação partidária ou sindical, estatuto migratório, conflitos fundiários e localização de pessoas vulneráveis.
11. **Dados geoespaciais pessoais:** coordenadas, polígonos, rotas, imagens ou atributos espaciais ligados a uma pessoa, agregado, parcela, estrutura ou actividade identificável.
12. **Anonimização:** transformação que impede de forma razoável e duradoura a reidentificação, considerando outros dados disponíveis. Dados pseudonimizados não são anónimos.
13. **Pseudonimização:** substituição de identificadores por um código, mantendo uma chave separada que permite reidentificação.
14. **Responsável pelo tratamento:** entidade que decide por que razão e como os dados são tratados.
15. **Processador:** entidade que trata dados por instrução documentada do responsável. A terminologia de diplomas locais pode diferir; o contrato deve mapear as funções e ser revisto juridicamente.
16. **Participante/respondente:** pessoa que fornece dados ou sobre quem são recolhidos dados.

2.3 Níveis de classificação

Nível	Exemplos	Regra mínima
Público	Indicadores agregados aprovados, metodologia publicada, mapas sem risco de reidentificação	Publicação autorizada e verificação de divulgação
Interno	Materiais de formação, cronogramas, formulários sem dados reais	Acesso a pessoal e parceiros autorizados
Confidencial	Microdados pseudonimizados, dados empresariais, contactos separados, resultados não publicados	Acesso por função, encriptação e partilha controlada
Restrito	Nomes ligados a saúde/VBG/crianças, GPS de domicílios, biometria, gravações reconhecíveis, chaves de ligação, casos de protecção	Aprovação de alto risco, acesso nominal, registo de acesso, encriptação reforçada e retenção curta

Se houver dúvida, a equipa deve usar a classificação mais alta até decisão do Gestor de Dados e do Responsável de Governança de Dados.

3. Princípios fundamentais

3.1 Não causar dano

A recolha só é justificável quando os benefícios informativos superam riscos previsíveis. A equipa avalia danos físicos, psicológicos, sociais, económicos, jurídicos, digitais e reputacionais, incluindo danos causados por reidentificação ou pela presença visível da equipa. Uma entrevista tecnicamente correcta deve ser interrompida se expuser o respondente a violência, estigma, retaliação ou perda de assistência.

3.2 Necessidade, proporcionalidade e minimização

Recolher apenas o que é necessário para uma pergunta e uma decisão definidas. Cada variável sensível deve ter justificação escrita. “Pode ser útil mais tarde” não é justificação. Sempre que um distrito, faixa etária ou código aleatório servir, não recolher endereço, data de nascimento exacta ou nome.

3.3 Finalidade determinada

Antes do contacto, a Data4Moz deve definir finalidade, utilizadores, produtos, prazo de retenção e formas de partilha. Nova finalidade exige avaliação de compatibilidade, autorização contratual e ética e, quando necessário, novo consentimento. Dados de monitoria não podem ser convertidos silenciosamente em pesquisa, marketing, vigilância, elegibilidade ou aplicação da lei.

3.4 Exactidão e integridade

A Data4Moz deve representar fielmente o que foi perguntado, observado e inferido. Não preencher respostas por suposição, não alterar dados para atingir metas e não apresentar informação declarada como verificada. Correções devem manter trilho de auditoria. A exactidão protege o participante contra decisões erradas e protege o cliente contra conclusões indefensáveis.

3.5 Transparência

O participante deve saber quem recolhe, para quem, porquê, o que acontecerá aos dados, que riscos existem e como reclamar. Não usar descrições vagas para esconder temas sensíveis. Limites de confidencialidade, como risco iminente ou obrigação legal confirmada, devem ser explicados antes da entrevista.

3.6 Justiça e inclusão

Não excluir pessoas por língua, deficiência, localização, género ou pobreza por conveniência da equipa. Não concentrar o peso da pesquisa em comunidades fáceis de alcançar. Adaptações razoáveis devem permitir participação segura, sem baixar os critérios de consentimento.

3.7 Responsabilidade demonstrável

Não basta cumprir; é necessário conservar prova de que os riscos foram avaliados, a equipa foi formada, o consentimento foi obtido, os acessos foram controlados, as reclamações foram tratadas e os dados foram eliminados no prazo.

4. Portão obrigatório antes do campo

O Gestor do Projecto não autoriza mobilização enquanto o Dossier de Conformidade do Projecto não contiver:

17. contrato e definição de responsável/processador, propriedade, partilha, devolução e eliminação;
18. objectivo, metodologia, população, amostra, critérios de inclusão e regras de substituição;
19. inventário de variáveis, classificação, fluxo de dados e localização dos servidores;
20. Avaliação de Impacto Ético e de Protecção de Dados para qualquer risco elevado;
21. confirmação de autorização do INE quando aplicável;
22. aprovação técnico-científica, ética, registo e autorizações de saúde quando aplicáveis;
23. aprovações administrativas, comunitárias e de aviação/drone pertinentes;
24. instrumentos, traduções, guiões de consentimento e plano de encaminhamento aprovados;

25. configuração segura de plataforma, contas, perfis, encriptação, cópia de segurança e teste de restauração;
26. plano de retenção, partilha, anonimização e destruição;
27. mecanismo de reclamação e materiais de contacto em línguas apropriadas;
28. formação, avaliação e certificação de cada membro da equipa;
29. piloto que confirme duração, privacidade, compreensão, risco e funcionamento técnico;
30. plano de segurança física, comunicação e evacuação para a área de trabalho.

NÃO AUTORIZAR: Se o cliente pedir dados identificáveis sem finalidade, base legal, segurança, prazo e acordo de partilha documentados, o Gestor do Projecto deve suspender a configuração e remeter o pedido à Direcção e ao responsável de governação de dados.

5. Entrada comunitária e sensibilidade cultural em Moçambique

5.1 Entrada respeitosa

As equipas devem seguir os canais administrativos e comunitários adequados. Dependendo do local, isso pode envolver autoridades provinciais ou distritais, posto administrativo, localidade, município, secretário de bairro, régulo, chefe tradicional, líder religioso ou comité comunitário.

1. Levar carta de credencial e explicar o projecto, entidade contratante, áreas, calendário, método de selecção, duração e contacto para reclamações.
2. Perguntar sobre língua, horários, segurança, acontecimentos comunitários e normas de visita.
3. Esclarecer que a liderança facilita a entrada, mas não escolhe respostas, não vê questionários e não consente pelas famílias.
4. Pedir que líderes não acompanhem entrevistas nem pressionem pessoas a participar.
5. Registar a reunião de entrada e qualquer condição acordada, sem registar informação política desnecessária.

Fazer: reconhecer a autoridade local, informar com antecedência e corrigir rumores. **Não fazer:** prometer projectos, pagamentos ou benefícios; pedir ao régulo uma lista de “boas famílias”; aceitar que um líder responda por toda a comunidade; exhibir listas de beneficiários.

5.2 Língua e tradução

O português não deve ser presumido como a língua preferida. A equipa prepara um mapa linguístico por local, considerando línguas como Emakhuwa, Xichangana, Cisena, Elomwe, Echuwabo, Cinyanja, Ciyao, Shimakonde, Kimwani, Cindau e outras variantes locais, sem assumir que uma província é linguisticamente uniforme.

6. Traduzir guiões e termos-chave com tradutor competente e revisor local independente.
7. Fazer retrotradução ou revisão por painel e teste cognitivo com pessoas semelhantes à população-alvo.
8. Manter glossário aprovado para consentimento, saúde, nutrição, VBG, posse da terra e escalas de resposta.
9. Não improvisar palavras sensíveis. Se o conceito não tiver equivalente directo, explicar com frase aprovada e registar a versão usada.
10. Não usar crianças, vizinhos, líderes ou membros da família como intérpretes de temas sensíveis. Intérpretes profissionais assinam confidencialidade.
11. Registar a língua da entrevista e dificuldades de compreensão para avaliar viés.

5.3 Género, idade e poder

Quando o tema for saúde sexual, VBG, protecção, rendimentos pessoais ou relações familiares, oferecer entrevistador do género preferido sempre que possível. Uma mulher adulta não necessita da autorização do marido para consentir. Contudo, a equipa deve avaliar risco de retaliação e nunca insistir numa entrevista que não possa ser privada.

Não presumir que o chefe do agregado conhece a experiência de todos. Entrevistar a pessoa seleccionada. Entrevistas por procuração só são permitidas pelo protocolo e devem ser marcadas como tal. Para adolescentes e crianças, aplicar consentimento do responsável e assentimento, além de privacidade apropriada e plano de salvaguarda.

5.4 Momento e conduta no agregado

Combinar horários que não prejudiquem trabalho, escola, mercado, machamba, pesca, recolha de água, oração, refeições, funerais, cerimónias ou descanso. Não entrevistar à noite salvo necessidade documentada, plano de segurança e pedido do participante. Pedir licença antes de entrar, sentar, fotografar ou tocar em bens. Procurar um local onde terceiros não ouçam. Manter tom neutro, vestuário apropriado e distância respeitosa. Não comentar condições da casa, práticas religiosas, relações familiares ou respostas. Não aceitar dinheiro. Qualquer compensação aprovada deve ser explicada de forma igual e não depender das respostas.

5.5 Respeitar normas sem comprometer a integridade

O respeito cultural não autoriza falsificação, substituição informal da amostra, exclusão de mulheres ou jovens, exposição de respostas ou omissão de consentimento. Se uma norma local colidir com segurança, direitos ou método, o enumerador não resolve sozinho: pausa, protege o participante e chama o supervisor. Toda adaptação deve ser documentada.

6. Selecção, contacto e qualidade no terreno

6.1 Recrutamento

12. Usar apenas listas autorizadas e transferidas com segurança.
13. Revelar ao mobilizador apenas a informação necessária para localizar a unidade, nunca respostas anteriores ou atributos sensíveis.
14. Não permitir que líderes, provedores de serviços ou empregadores observem quem aceitou ou recusou.
15. Explicar como a pessoa foi seleccionada sem sugerir que a participação é condição para benefícios.
16. Não substituir um agregado ausente ou recusante por um vizinho. Seguir as revisitas e substituições aprovadas e obter autorização do supervisor.
17. Obter consentimento separado para contacto de seguimento ou verificação posterior.

6.2 Durante a entrevista

O enumerador lê perguntas conforme o instrumento, usa sondagens neutras, respeita “não sei” e “prefiro não responder”, e regista observação separada de resposta declarada. Não aconselhar a resposta, não completar perguntas sem resposta e não copiar uma entrevista anterior. O enumerador deve interromper quando:

18. o participante retira consentimento ou demonstra que não compreende;
19. não há privacidade para tema sensível;
20. chega pessoa cuja presença cria risco;
21. o participante está em sofrimento, intoxicado, gravemente doente ou sob ameaça;
22. uma criança recusa, mesmo com consentimento do adulto;

- 23. o dispositivo, formulário ou selecção está errado;
- 24. alguém exige acesso às respostas;
- 25. existe perigo físico para participante ou equipa.

6.3 Controlo de qualidade ético

Supervisores podem usar duração, trajecto, padrões de resposta e back-checks autorizados para detectar erro. Esses sinais não provam fraude isoladamente. A confirmação deve ser justa, confidencial e documentada. Gravação de áudio, fotografia silenciosa ou localização contínua para controlo de enumeradores ou respondentes exige aviso, necessidade e consentimento apropriado; não pode ser activada por defeito.

7. Consentimento informado

7.1 Condições de consentimento válido

Consentimento é considerado um processo, e não uma assinatura. O processo deve ser informativo, específico, compreensível, voluntário e administrado por uma pessoa com capacidade. Deve ocorrer antes da recolha e permanecer válido durante a actividade. O participante deve receber, em língua e formato compreensíveis:

- 26. identidade da Data4Moz, cliente e contactos;
- 27. finalidade e razão da selecção;
- 28. actividades, duração e temas;
- 29. riscos, desconfortos e benefícios, incluindo ausência de benefício directo;
- 30. compensação ou reembolso, se houver;
- 31. dados recolhidos, utilização, destinatários, país/servidor quando relevante e prazo;
- 32. medidas e limites da confidencialidade;
- 33. elementos opcionais, como gravação, fotografia, GPS e contacto futuro;
- 34. direito de recusar perguntas, recusar o estudo ou retirar-se sem penalização e sem perda de benefícios;
- 35. como solicitar acesso, correcção, retirada quando possível, ou apresentar reclamação.

Usar uma pergunta de confirmação: “Pode dizer-me, por suas palavras, o que acontece se decidir não participar?” Se a resposta revelar incompreensão, voltar a explicar. Não transformar a confirmação num exame nem envergonhar a pessoa.

7.2 Recusa e retirada

Uma recusa encerra o contacto com respeito. Não se deve solicitar o motivo salvo pergunta opcional aprovada. Não enviar líder, beneficiário ou outro enumerador para persuadir. Na retirada, parar a recolha e perguntar se o participante permite conservar o que já foi recolhido. Explicar previamente que dados já anonimizados e não rastreáveis podem não ser retirados.

7.3 Baixa literacia e consentimento oral

Quando a pessoa não sabe ler, o enumerador lê o texto integral, disponibiliza tempo para perguntas e documenta consentimento oral. Se o protocolo exigir testemunha, esta deve ser adulta, independente da equipa e, de preferência, não ser líder, provedor de benefício ou pessoa com poder sobre o participante.

O registo deve conter versão do guião, data/hora, código do participante, língua, nome/código do enumerador, método oral, resultado da verificação de compreensão e código da testemunha. Impressão digital só é recolhida se exigida e aprovada; é identificador biométrico e não deve ser usada como solução automática para analfabetismo.

7.4 Crianças e menores

Para menores de 18 anos, a regra da Data4Moz é consentimento de pai/mãe ou responsável legal e assentimento da criança adequado à idade e maturidade. A recusa da criança prevalece. Excepções para menores emancipados, serviços confidenciais de adolescentes ou impossibilidade de obter autorização só podem ocorrer com base legal e aprovação ética documentadas.

Não entrevistar criança diante de pessoa que possa influenciar respostas, mas cumprir o plano aprovado de supervisão e salvaguarda. Não prometer sigilo absoluto se o protocolo prevê acção perante risco imediato de dano. Explicar esse limite de modo simples antes de perguntar.

Para adultos com capacidade de decisão reduzida, não presumir incapacidade por deficiência, idade, escolaridade ou língua. Usar apoio de comunicação e avaliação prevista no protocolo. Representante legal e assentimento da pessoa são necessários quando a capacidade estiver efectivamente comprometida.

7.5 Consentimentos separados

Participação, fotografia, vídeo, áudio, citação atribuída, GPS exacto, drone, contacto futuro e uso público são decisões distintas. Uma caixa pré-seleccionada ou um único “aceito tudo” não é consentimento específico. Se GPS for essencial ao método, informar que a pessoa pode recusar a actividade inteira sem consequência; não dizer que pode continuar se isso não for verdade.

8. Saúde, nutrição, VBG, protecção e outros temas sensíveis

8.1 Triagem obrigatória

O projecto exige Avaliação de Impacto Ético e de Protecção de Dados, revisão especializada e, quando aplicável, aprovação ética externa se envolver saúde individual, crianças, VBG, violência, exploração, tráfico, HIV, saúde mental, deficiência, biometria, amostras biológicas, actividade ilegal, conflito fundiário, deslocados, refugiados, minorias, localização de espécies ameaçadas ou qualquer consequência adversa plausível.

8.2 Saúde e nutrição

Estudos de saúde humana podem estar sujeitos à Lei n.º 6/2023 e ao Decreto n.º 53/2024. O código “M&A” não elimina a obrigação quando a actividade constitui investigação em saúde humana. O Gestor do Projecto poderá obter determinação escrita do cliente ou parceiro, INS/CNBS ou jurista quando houver dúvida.

Medições antropométricas exigem equipamento calibrado, higiene, privacidade, consentimento específico, procedimento para roupa e contacto físico, e formação prática. Enumeradores não diagnosticam nem prometem tratamento. Resultados clinicamente relevantes só são comunicados conforme protocolo validado, com encaminhamento realista e sem criar falsa garantia de serviço.

8.3 Violência baseada no género e protecção

Recolha de dados sobre violência só ocorre se a informação for necessária, a equipa tiver formação especializada, a privacidade puder ser assegurada e existirem procedimentos de segurança e encaminhamento verificados. Aplicam-se as recomendações da OMS para colocar a segurança da participante em primeiro lugar.

36. Usar título e materiais neutros que não revelem o tema.
37. Entrevistar apenas uma pessoa elegível por agregado quando o protocolo o exigir.
38. Não realizar a entrevista com parceiro, familiar, líder ou criança presente.
39. Preparar pergunta de mudança rápida para tema neutro se alguém se aproximar.
40. Não guardar nome, número e relato de violência no mesmo ficheiro.

41. Não inserir local exacto em relatórios de caso nem enviar caso por WhatsApp.
42. Não confrontar alegado agressor nem investigar além do mandato.
43. Oferecer informação de apoio de modo discreto e apenas para serviços confirmados.
44. Explicar obrigações de denúncia que tenham sido juridicamente confirmadas. Nunca inventar uma obrigação nem prometer que nenhuma comunicação será feita.

Se não houver privacidade, cancelar ou remarcar. Completar a meta amostral não justifica expor uma pessoa.

8.4 Crianças e salvaguarda

Todo projecto com crianças tem um ponto focal de salvaguarda, código de conduta, regras de contacto, canais de denúncia e mapa de serviços. Nenhum membro fica sozinho com uma criança em local isolado. Não recolher histórias traumáticas apenas para ilustrar um relatório. Identidade, escola, imagem e localização de criança em caso de protecção são dados restritos.

8.5 Agricultura, terra, meios de vida e conservação

Informação sobre posse, limites de parcelas, acesso a água, rendimentos, práticas informais, recursos naturais e conflitos pode afectar direitos ou fiscalização. Não prometer que o mapeamento reconhece título, resolve conflito ou garante assistência. Mapas participativos devem mostrar desacordos e fontes, não converter a opinião da pessoa mais influente em “verdade comunitária”. Locais sagrados, rotas de uso, recursos raros e espécies ameaçadas não devem ser publicados com precisão que permita exploração ou dano.

9. GPS, fotografia, áudio, vídeo, imagens e drones

9.1 GPS

Antes de activar localização, definir por que é necessária, precisão mínima, duração, acesso e produto final. Preferir centróide, unidade administrativa, grelha ou ponto deslocado quando o endereço exacto não for necessário.

45. Mostrar ou explicar que a coordenada pode revelar residência, parcela, local de trabalho ou rota.
46. Guardar a ligação entre código e coordenada em ficheiro restrito e separado.
47. Desactivar rastreio contínuo, histórico de localização e metadados não necessários.
48. Não publicar pontos de domicílios. Aplicar agregação, generalização ou deslocamento e testar reidentificação com estradas, imagens e listas públicas.
49. Não usar coordenada recusada ou inválida inventando ponto no escritório.

9.2 Fotografia, áudio e vídeo

Obter consentimento separado para cada uso: prova interna, análise/transcrição, relatório do cliente, formação ou comunicação pública. A pessoa deve poder participar sem aparecer em fotografia, salvo se a imagem for a própria actividade e isso tiver sido explicado antes da selecção.

Não fotografar formulários, cartões, ecrãs, crianças, doentes, sobreviventes, casas ou bens sem autorização. Remover geotags quando desnecessárias. Armazenar em aplicação aprovada, não na galeria pessoal nem em cópia automática para nuvem. Uma face ou voz reconhecível continua pessoal mesmo sem nome.

9.3 Drones e imagens aéreas

Nenhum voo pode ser efectivado sem confirmação escrita dos requisitos actuais do Instituto de Aviação Civil de Moçambique, autorizações de espaço aéreo e local, qualificação do operador,

seguro e avaliação de segurança. A equipa deve confirmar o instrumento vigente; esta versão não afirma um número de directiva de RPAS¹ que não foi possível verificar numa fonte oficial acessível. Autorização de voo não resolve privacidade. Informar a comunidade sobre área, horário, finalidade, sensores e contacto; evitar voar sobre pessoas, pátios e actividades privadas; planejar resolução e ângulo que reduzam identificação; aplicar máscara a faces, matrículas e propriedades quando necessário. Imagem aérea original é restrita até revisão. O uso secundário exige nova avaliação.

10. Procedimentos por meio de recolha

10.1 KoboToolbox/ODK

50. Conta individual, palavra-passe forte e autenticação multifactor quando disponível.
51. Formulário encriptado com chave gerida pela organização para dados confidenciais/restritos.
52. Direitos mínimos: enumerador envia; supervisor revê apenas a sua equipa; exportação limitada ao Gestor de Dados.
53. Desactivar edição, anexos, auditoria, identificação de dispositivo ou localização quando não necessários.
54. Testar saltos, restrições, cálculo, idiomas, repetição, modo offline e cenário de perda de ligação.
55. Sincronizar apenas com servidor aprovado; confirmar recepção antes de apagar cópia local.
56. Não colocar identificadores ou dados reais em nomes de ficheiros, notas de suporte ou mensagens.

10.2 ArcGIS Survey123 e Field Maps

57. Usar contas nomeadas, grupos privados, MFA e princípio do menor privilégio.
58. Feature layers, mapas web e anexos ficam privados por defeito; impedir links públicos.
59. Limitar edição, exportação, partilha e sincronização offline por função.
60. Separar camada identificável da camada analítica; usar vistas alojadas com campos reduzidos.
61. Testar áreas offline, conflitos de sincronização, precisão e eliminação do dispositivo.
62. Não publicar mapa de campo nem dashboard antes de revisão de divulgação.

10.3 Dispositivos

De preferência usar equipamento próprios da organização. Exigir sistema suportado, encriptação integral, PIN de seis ou mais dígitos, bloqueio automático após um tempo, actualizações, localização/eliminação remota e inventário. Proibir partilha de contas, root/jailbreak, instalação não autorizada, capturas de ecrã e cópia automática de fotografias.

Nunca deixar dispositivo em locais inseguros, emprestar a participante ou transportar sem controlo. Uma perda ou suspeita de acesso deve ser comunicada imediatamente, mesmo se o equipamento estiver encriptado.

10.4 Papel

63. Usar código, não nome, no questionário sempre que possível; consentimento e lista de ligação viajam separados.
64. Numerar formulários e manter registo diário de emissão, devolução e páginas.
65. Transportar em pasta fechada; guardar em armário com chave e acesso registado.

¹ Remotely Piloted Aircraft System

66. Não deixar formulários em casas, hotéis, viaturas ou secretarias locais.
67. Digitalizar em ambiente controlado com dupla verificação; não fotografar com telefone pessoal.
68. Registrar transferência e destruição. Destruir por trituração segura ou método aprovado, com testemunho e certificado.

11. Utilização, partilha, retenção e eliminação de dados

11.1 Limitação de uso

Os dados são usados apenas para a finalidade explicada e documentada. Ligação com novas bases, perfilagem, inteligência artificial, reconhecimento facial, marketing, avaliação de elegibilidade ou publicação de casos individuais exige revisão e aprovação interna. Uma base de dados recebida do cliente não se torna automaticamente propriedade de uso geral da Data4Moz.

11.2 Partilha

Por defeito, clientes recebem resultados agregados e microdados desidentificados. Dados identificáveis só são transferidos quando necessários, autorizados pelo contrato, cobertos pelo consentimento ou outra base legal válida, e protegidos por Acordo de Partilha/Tratamento de Dados.

O acordo deve definir finalidade, campos, funções, local de armazenamento, segurança, utilizadores, transferência internacional, subcontratados, proibição de uso ulterior e reidentificação, incidente, auditoria, prazo e prova de eliminação. Não é permitido encaminhamento a terceiro sem autorização escrita.

Pedidos de autoridade, polícia, tribunal ou entidade pública são encaminhados à Direcção e ao jurista. O enumerador nunca entrega dispositivo, lista ou resposta por iniciativa própria. A Data4Moz verifica competência, forma do pedido e possibilidade de limitar a divulgação ao mínimo legal.

11.3 Transferência segura

Usar portal aprovado, SFTP², repositório com acesso temporário ou outro canal encriptado. Não usar correio electrónico aberto, WhatsApp, pen drive não encriptada ou link público. Confirmar destinatário por canal separado, definir expiração, limitar downloads e registar entrega.

11.4 Calendário de retenção por defeito

O calendário do projecto prevalece se for juridicamente válido e mais protector. Na ausência de obrigação diferente, usar estes máximos e eliminar mais cedo quando a finalidade terminar:

Registo	Máximo recomendado	Acção final
Lista de contacto/recrutamento	90 dias após validação do campo	Eliminar com registo
Chave nome-código e GPS exacto	90 dias após QA e aceitação, salvo seguimento aprovado	Eliminar ou separar para seguimento autorizado
Áudio/vídeo para transcrição ou QA	30 dias após transcrição/QA, máximo 90 dias	Eliminação segura
Microdados identificáveis	12 meses após aceitação final	Anonimizar ou eliminar
Microdados pseudonimizados de análise	24 meses após encerramento	Anonimizar ou eliminar
Consentimento e prova de aprovação	Prazo contratual/ético; por defeito 5 anos, com dados mínimos	Arquivo restrito e eliminação segura
Dados restritos de	Prazo aprovado, normalmente mais curto	Eliminar segundo aprovação ética

² Secure File Transfer Protocol

VBG/protecção/criança	que dados gerais	
Papel digitalizado e validado	Máximo 90 dias, excepto consentimento	Destruição certificada
Dados verdadeiramente anónimos e indicadores	Conforme valor institucional e licença	Arquivo governado

Não aplicar automaticamente a dados de inquérito prazos de retenção previstos para tráfego de telecomunicações ou prova criminal. O jurista deverá confirma qualquer obrigação específica.

11.5 Eliminação

Eliminar cópias activas, offline, de exportação, temporárias e de dispositivos. As cópias de segurança devem seguir um ciclo documentado e tornam-se inacessíveis fora de restauração. Para armazenamento encriptado, poderá se usar eliminação criptográfica aprovada. Registrar data, conjunto, método, responsável e verificador. Se o cliente deve eliminar, pedir certificado.

12. Anonimização e divulgação responsável

1. Remover identificadores directos: nome, telefone, BI, endereço, fotografia, voz e identificadores de plataforma.
2. Separar e proteger a chave de ligação.
3. Tratar identificadores indirectos: idade exacta, datas, profissão rara, composição familiar, escola, aldeia, empregador e eventos únicos.
4. Rever texto livre, anexos, nomes de ficheiro e metadados.
5. Reduzir precisão espacial por agregação, grelha, generalização ou deslocamento que respeite fronteiras; testar contra imagens, estradas e dados públicos.
6. Avaliar combinações raras e inferência de atributos sensíveis. Métricas como k-anonimato ajudam, mas não garantem anonimato.
7. Aplicar supressão de células. Por defeito, não publicar contagens inferiores a 5; usar limiar de 10 ou agregação adicional para crianças, VBG, saúde rara ou localizações pequenas, salvo avaliação aprovada.
8. Fazer revisão independente de divulgação antes de entregar ou publicar.

Não chamar “anónimo” a conjunto que conserva códigos reidentificáveis, GPS exacto ou narrativas reconhecíveis. Dados sintéticos e mapas com pontos deslocados também exigem teste de risco.

13. Privacidade e segurança ao longo do ciclo de vida

13.1 Em trânsito e armazenamento

Todos os dados confidenciais/restritos devem usar encriptação em trânsito e em repouso. Documentar fornecedor, região de alojamento, subcontratados, cópias, recuperação, acesso administrativo e transferência transfronteiriça. Acesso é concedido por nome e função, aprovado pelo proprietário do dado, revisto durante o projecto e removido no mesmo dia da saída da equipa.

13.2 Durante a análise

Analistas de dados trabalham em espaço aprovado, com dados minimizados e pseudonimizados. Não copiar para computador pessoal, correio, aplicações de mensagens ou serviços de IA generativa sem avaliação, acordo e autorização. Exportações devem ser numeradas, justificadas e eliminadas. Resultados, tabelas, citações e mapas passam por controlo de divulgação.

13.3 Cópias de segurança e continuidade

Manter cópias encriptadas proporcionais ao risco, separadas do ambiente principal, com acesso restrito. Testar restauração e documentar resultado. Uma cópia de segurança não deve tornar-se arquivo sem prazo.

13.4 Credenciais e suporte

Não partilhar palavra-passe. MFA³ é obrigatório para contas com exportação, administração ou dados restritos. Incidentes de suporte não devem incluir dados reais salvo canal aprovado e mínimo necessário. Revogar tokens, chaves e ligações temporárias após uso.

14. Incidentes de dados e violações

14.1 O que deve ser comunicado

Perda ou roubo de dispositivo/papel; envio ao destinatário errado; link público; conta comprometida; malware; acesso indevido; captura de ecrã; sincronização para nuvem pessoal; revelação durante entrevista; publicação de ponto identificável; destruição ou alteração não autorizada; incapacidade de localizar ficheiro; ou suspeita razoável.

14.2 Acção imediata

1. Proteger pessoas e interromper a exposição.
2. Comunicar ao supervisor e canal de incidentes imediatamente, idealmente na primeira hora. Não esperar confirmação.
3. Desligar ligação ou revogar acesso quando seguro, sem apagar prova ou alterar registos.
4. Anotar hora, dados, dispositivo, pessoas, acções e possíveis afectados.
5. Seguir instruções para bloqueio remoto, preservação, mudança de credenciais e contacto com fornecedor.
6. Não contactar participantes, imprensa, polícia ou cliente fora do plano de resposta.

O Responsável de Segurança e o Responsável de Governação de Dados fazem avaliação inicial em 24 horas: tipo e volume, sensibilidade, encriptação, acesso provável, consequências, jurisdições, contrato e medidas. O Gestor do Projecto notifica cliente/controlador sem demora indevida e cumpre prazo contratual. Se o RGPD se aplicar, a decisão sobre notificação à autoridade em 72 horas e aos titulares é tomada pelo responsável, com assessoria jurídica. As Leis n.º 13/2026 e 14/2026 e regulamentos podem impor notificação ao CSIRT; confirmar a sua entrada em vigor e prazos.

Depois: conter, recuperar, investigar causa, apoiar afectados, aplicar correcção, documentar decisão de notificar ou não e rever controlos. A comunicação precoce de boa-fé não deve ser punida.

15. Funções e responsabilidades

Função	Responsabilidades essenciais
Direcção	Aprovar política, nomear responsáveis, fornecer recursos, aceitar risco residual e assegurar revisão jurídica
Gestor do Projecto	Definir finalidade e funções contratuais, completar portão de conformidade, obter aprovações, garantir recursos e suspender trabalho inseguro
Responsável de Governação/Protecção de Dados	Avaliar impacto, rever consentimento e partilha, manter registos, tratar direitos e reclamações, apoiar incidentes
Responsável de Segurança da Informação/CSIRT	Configuração, acessos, risco cibernético, monitoria, resposta, cópias e preparação para a Lei n.º 13/2026
Auditor Interno de Segurança	Verificação independente dos controlos e seguimento de correcções; não deve auditar apenas o próprio trabalho
Gestor de Dados	Dicionário, classificação, plataforma, qualidade, pseudonimização, exportações, retenção e eliminação
Coordenador de Campo	Entrada comunitária, logística segura, escala linguística e de género, reclamações e incidentes físicos

³ Multifactor Authentication

Supervisor	Observação, apoio, revisão diária, autorização de revisitas/substituições, cadeia de custódia e escalonamento
Enumerador/Intérprete	Consentimento, privacidade, aplicação fiel, segurança do dispositivo/papel, comunicação imediata e respeito
Analista	Minimização, ambiente aprovado, análise reproduzível, controlo de divulgação e eliminação de exportações
Subcontratado/Parceiro	Mesmas obrigações, acordo escrito, formação, acesso limitado e prova de eliminação

Nenhuma pessoa aprova sozinha uma excepção que beneficie o seu prazo ou entrega. Alto risco requer pelo menos Gestor do Projecto, Governação de Dados e responsável técnico/sectorial; questões legais exigem jurista.

16. Formação, supervisão e conduta

Antes do acesso, cada pessoa conclui formação geral e específica do projecto, assina confidencialidade e código de conduta e demonstra competência por teste e simulação. A nota recomendada é 70%, com nova formação antes de repetir. Temas obrigatórios: ética, consentimento, língua, amostra, privacidade, plataformas, segurança, incidentes, reclamações, prevenção de exploração e abuso sexual, e salvaguarda. VBG, crianças, saúde, antropometria, biometria e drones exigem módulos e prática especializados. Participar numa formação geral não qualifica para essas tarefas.

Supervisores fazem reunião diária, verificam consentimento e desvios, observam entrevistas apenas com autorização, revêem métricas sem expor respostas e registam acções correctivas. A Direcção realiza auditorias de projecto e amostras de conformidade. Fraude, coerção, divulgação intencional ou retaliação podem levar a retirada imediata do campo e processo disciplinar, com apuramento justo.

17. Reclamações, direitos e reparação

Cada participante recebe cartão ou informação oral com código do projecto e canais gratuitos ou de baixo custo: telefone/SMS, correio electrónico, contacto local e endereço. Deve existir alternativa fora da linha do supervisor para reclamação sobre a equipa. Campos a preencher antes do campo:

7. Telefone/SMS da Data4Moz: **Dependendo do projecto**
8. Correio electrónico: admin@data4moz.com
9. Ponto focal de ética/salvaguarda: **Dependendo do projecto**
10. Canal independente do cliente/doador, se aplicável: **Quando aplicável**

Aceitar reclamação anónima e em língua local. Registrar apenas o necessário, confirmar recepção em dois dias úteis, classificar risco, encaminhar salvaguarda imediatamente e procurar resolver em 15 dias úteis ou informar novo prazo. Proibir retaliação e não retirar benefício. Pedidos de acesso, correcção ou eliminação são verificados com cuidado para não revelar dados a pessoa errada. Quando a Data4Moz causar dano, deve considerar correcção, retirada de publicação, aviso, apoio, reposição de custo ou outra reparação proporcional, sem exigir renúncia indevida de direitos.

18. Quadro jurídico e normativo

18.1 Moçambique: instrumentos confirmados e pontos a verificar

Instrumento/estado em 16-08-2026	Relevância operacional	Acção Data4Moz
Constituição da República, versão consolidada até Lei n.º 1/2018; arts. 41, 68 e 71	Privacidade, imagem, inviolabilidade do domicílio/comunicação; restrições a dados identificáveis sobre crenças, religião, filiação e vida	Entrada e consentimento individual; revisão jurídica obrigatória antes de recolher categorias do art. 71; processo de acesso/correcção

	privada; acesso e rectificação	
Lei n.º 3/2017, de 9 de Janeiro, Transacções Electrónicas; arts. 63-65	Finalidade prévia, exactidão, confidencialidade, segurança, direitos, proibição de acesso/transfêrencia não autorizada e responsabilidade do processador	Aplicar a toda recolha electrónica e nomear função responsável; publicar informação de contacto/política
Resolução n.º 5/2019 e Convenção da UA sobre Cibersegurança e Protecção de Dados Pessoais	Moçambique ratificou; Convenção entrou em vigor em 8-06-2023	Alinhar princípios e confirmar com jurista o efeito directo/domesticação em cada questão
Proposta de Lei de Protecção de Dados Pessoais	Actualização oficial de 17-06-2026 indicava apreciação parlamentar; não foi localizada publicação oficial de lei aprovada até a data de corte	Não citar a proposta como lei. Monitorar AR/INM/INTIC e rever política na aprovação
Lei n.º 13/2026, de 1 de Julho, Segurança Cibernética	Publicada com entrada em vigor 90 dias depois; prevê política, risco, formação, responsável, auditor interno, CSIRT e notificação para sector privado; vários detalhes dependem de regulamento	Plano de transição antes da vigência; jurista confirma data exacta, enquadramento e regulamentos; nomeações formais pela Direcção
Lei n.º 14/2026, de 1 de Julho, Crimes Cibernéticos	Criminaliza acesso, interceptação e interferência não autorizados; também com vigência diferida	Autorização escrita, contas individuais, preservação de prova e resposta jurídica
Lei n.º 7/96 e Decreto n.º 34/98, Sistema Estatístico Nacional	Autorização prévia do INE para inquéritos por serviços do Estado, autarquias e entidades públicas ou com funções de interesse público; segredo estatístico nas estatísticas oficiais	Triagem em todos os inquéritos ligados a Governo/interesse público; obter autorização/posição escrita do INE; não afirmar autoridade estatística sem mandato
Lei n.º 6/2023 e Decreto n.º 53/2024, Investigação em Saúde Humana	Aprovação técnico-científica, revisão ética, registo e regulação por INS/CNBS e comités acreditados, conforme actividade	Determinar se saúde/nutrição/M&A constitui investigação; obter aprovações antes do recrutamento
Lei n.º 7/2008, Promoção e Protecção dos Direitos da Criança; Convenção sobre os Direitos da Criança	Melhor interesse, privacidade, protecção e participação da criança; menor de 18 anos como regra	Consentimento do responsável, assentimento, salvaguarda e minimização, salvo excepção legal/ética
Lei n.º 34/2014 e Decreto n.º 35/2015, Direito à Informação	Pode abranger privados com actividade/recursos de interesse público, mas protege dignidade e vida privada	Coordenar pedidos com cliente e jurista; não publicar microdados pessoais como “informação pública”
Requisitos de RPAS/IACM	Requisitos exactos e instrumento vigente não foram confirmados numa fonte oficial acessível durante esta revisão	Confirmar por escrito com IACM antes de cada campanha, além de privacidade e autorizações locais

18.2 Normas internacionais e de financiadores

O RGPD⁴ aplica-se quando o seu âmbito territorial ou uma obrigação contratual o activar, não simplesmente porque um doador é europeu. O projecto deve documentar o gatilho. Quando aplicável: princípios e responsabilização (art. 5), base de licitude e consentimento (arts. 6-7), categorias especiais (art. 9), contratos responsável-processador (art. 28), segurança (art. 32), incidentes (arts. 33-34), avaliação de impacto (art. 35) e transferências internacionais (Capítulo V). A Data4Moz usa como referências reconhecidas: [Manual do CICV](#)⁵ sobre Protecção de Dados na Acção Humanitária, 3.ª edição; [Orientação Operacional do IASC](#) sobre Responsabilidade de Dados, revista em 2023; [Directrizes de Responsabilidade de Dados da OCHA](#), actualizadas em Janeiro de

⁴ Regulamento de Gestão e Protecção de Dados

⁵ Comitê Internacional da Cruz Vermelha

2025; orientações éticas da OMS⁶ para investigação sobre violência; [Diretrizes Éticas do UNEG](#); e política/procedimentos da UNICEF para actividades de evidência envolvendo pessoas, incluindo crianças.

Para cada parceiro ou cliente, o Gestor do Projecto extrai do contrato: aprovação ética, localização/transferência, prazo de incidente, titularidade, acesso, publicação, arquivo, auditoria, salvaguarda e eliminação. O requisito é anexado ao Plano de Responsabilidade de Dados e incluído na formação.

19. Monitoria, exceções e encerramento

Indicadores de conformidade incluem percentagem de pessoal certificado, projectos com avaliação de impacto, autorizações antes do campo, contas com MFA, incidentes e tempo de resposta, reclamações e resolução, acessos revogados, dados eliminados e certificados de destruição.

Excepção deve ser escrita, limitada no tempo, justificada, avaliada quanto a risco, aprovada por funções independentes e acompanhada de controlos compensatórios. Nunca se concede excepção a voluntariedade, proibição de coerção, salvaguarda de criança, proibição de falsificação ou comunicação de incidentes.

O encerramento exige reconciliação de dispositivos e papel, validação de sincronização, revogação de contas, devolução ao cliente, desidentificação, eliminação de temporários, confirmação de subcontratados, arquivo do dossier de conformidade, relatório de incidentes/reclamações e data da próxima eliminação.

⁶ Organização Mundial de Saúde

Anexo A. Cartão de bolso do enumerador

Antes de sair

11. Credencial, contactos de emergência e reclamação.
12. Dispositivo carregado, actualizado, bloqueado e formulário correcto.
13. Língua, amostra, rota, privacidade e encaminhamento revistos.
14. Sem dados desnecessários, cópias pessoais ou formulários antigos.

Em cada contacto

1. Apresentar-se e confirmar pessoa seleccionada.
2. Procurar privacidade e língua adequada.
3. Ler consentimento, verificar compreensão e registar decisão.
4. Perguntar sem induzir; aceitar recusa e pausa.
5. Obter consentimentos separados para GPS/media/contacto futuro.
6. Rever formulário sem dizer respostas em voz alta.
7. Agradecer, dar contacto e sair com segurança.

Pare e ligue ao supervisor

Sem consentimento; falta de privacidade; criança recusa; sofrimento; ameaça; líder exige respostas; formulário errado; GPS/foto não autorizado; dispositivo/papel perdido; promessa de benefício; desvio de amostra.

Anexo B. Guião-base de consentimento oral para adulto

“Bom dia/boa tarde. Chamo-me **[nome]** e trabalho com a Data4Moz. Estamos a realizar **[nome/descrição clara do projecto]** para **[cliente]**. O objectivo é **[finalidade]**. Foi seleccionado(a) através de **[método simples]**. Se aceitar, farei perguntas sobre **[temas]**. A conversa dura cerca de **[tempo]**. **[Explicar medição, observação ou acesso a registo.]** Algumas perguntas podem ser pessoais ou desconfortáveis. Pode não responder, pedir pausa ou terminar a qualquer momento. Participar é voluntário. Recusar não altera qualquer serviço, emprego, assistência ou benefício que receba agora ou no futuro.

Não prometemos benefício directo. **[Explicar compensação/reembolso ou dizer que não existe.]** Guardaremos os seus dados **[como/onde em termos compreensíveis]** e limitaremos o acesso à equipa autorizada. Os resultados serão apresentados **[de forma agregada/desidentificada]**. **[Explicar limites reais da confidencialidade.]** Conservaremos os dados identificáveis até **[data/período]** e depois serão eliminados ou anonimizados. **[Explicar partilha e país, se relevante.]** Pode contactar **[canal]** para perguntas, reclamações ou pedido sobre os seus dados. Antes de decidir, que perguntas tem? Pode dizer-me pelas suas palavras o que acontece se decidir não participar? **[Reexplicar se necessário.]** Aceita participar?”

Registo: sim/não; data/hora; código; versão; língua; enumerador; método escrito/oral; testemunha se exigida; confirmação de compreensão.

Anexo C. Guião-base de assentimento para criança/adolescente

“Olá. Chamo-me **[nome]**. Estamos a conversar com crianças/jovens para compreender **[explicação simples]**. Se quiseres participar, vou **[actividade]** durante cerca de **[tempo]**. Não é teste e não há resposta certa. Podes dizer que não, saltar qualquer pergunta ou parar. Ninguém vai retirar um serviço ou benefício por causa da tua decisão. **[Explicar privacidade e limite de segurança.]** O teu/tua responsável autorizou que te convidássemos, mas a decisão também é tua. Queres fazer perguntas? Queres participar?”

Se a criança disser não, ficar em silêncio por medo, se afastar ou mostrar oposição persistente, parar. Não pedir ao responsável que a convença.

Anexo D. Consentimento adicional para GPS, gravação e imagem

GPS opcional: “Gostaríamos de registar a localização aproximada deste [agregado/parcela/activo] para [finalidade]. A coordenada pode revelar onde fica. Não publicaremos o ponto exacto e o acesso será limitado. Pode recusar esta parte e continuar a entrevista. Autoriza?”

GPS essencial: “A localização é necessária para [razão]. Se não autorizar, não poderemos usar esta entrevista, mas a recusa não terá consequência nos seus serviços ou benefícios. Autoriza?”

Áudio: “Gostaríamos de gravar o áudio para [transcrição/qualidade]. Apenas [funções] ouvirão e apagaremos até [data]. Pode recusar e [continuar/não continuar, conforme protocolo]. Autoriza?”

Imagem: Registar escolhas separadas: prova interna; relatório restrito do cliente; formação; comunicação pública; identificação por nome; imagem de criança com assentimento. Não presumir que uma autorização abrange todas.

Anexo E. Triagem de Avaliação de Impacto

Se qualquer resposta for “sim” ou “incerto”, encaminhar para avaliação completa antes do campo:

8. Crianças, capacidade reduzida, deslocados, sobreviventes ou dependência de assistência.
9. Saúde, HIV, VBG, protecção, biometria, actividade ilegal, política/religião ou vida íntima.
10. Nomes ligados a dados sensíveis, GPS exacto, áudio, vídeo ou drone reconhecível.
11. Decisão sobre benefício, emprego, fiscalização, sanção ou encaminhamento.
12. Ligação de bases, IA, perfilagem, reconhecimento ou previsão individual.
13. Transferência internacional, fornecedor novo ou acesso de terceiro.
14. Grande escala, localização pequena, população rara ou risco de conflito.
15. Ausência de serviço de encaminhamento, privacidade ou canal de reclamação.
16. Nova finalidade, publicação aberta ou retenção longa.

A avaliação completa descreve necessidade, pessoas afectadas, fluxo, dano, probabilidade, controlos, risco residual, consulta, decisão e responsáveis.

Anexo F. Lista de verificação para partilha

17. Destinatário e identidade confirmados.
18. Finalidade compatível e campo a campo necessário.
19. Funções responsável/processador e base legal documentadas.
20. Consentimento/aprovação cobre a partilha.
21. Anonimização ou minimização feita e revista.
22. Acordo assinado, incluindo proibição de reidentificação e encaminhamento.
23. Transferência internacional e fornecedor revistos.
24. Canal encriptado, expiração e acesso nominal.
25. Prazo, eliminação e prova definidos.
26. Registo de quem enviou, recebeu, quando e qual versão.

Anexo G. Ficha de incidente

Registar: número; descobridor; data/hora; local/sistema; descrição factual; categorias e volume; classificação; encriptação; pessoas afectadas; exposição provável; medidas imediatas; contactos; cliente/controlador; jurisdições; prazos; decisão de notificação; apoio a afectados; causa; correcção; encerramento e aprovação. Não copiar dados pessoais para a ficha além do necessário.

Anexo H. Verificação do supervisor

27. Credenciais e consentimento observados correctamente.

28. Privacidade, língua e género adequados.
29. Amostra/revisita/substituição conforme regra.
30. Nenhuma promessa, coerção ou líder presente.
31. GPS, media e contacto futuro com decisão separada.
32. Sincronização, papel e dispositivos reconciliados.
33. Erros, recusas, sofrimento, reclamações e incidentes escalados.
34. Exportações e acessos desnecessários removidos.

Anexo I. Dossier de conformidade e encerramento

O dossier contém: contrato/DPA; parecer jurídico; autorização INE; aprovação ética/saúde; autorizações locais e IACM; avaliação de impacto; instrumentos e traduções; piloto; formação e avaliações; matriz de acesso; configurações; registos de consentimento; cadeia de custódia; QA; incidentes; reclamações; acordos de partilha; versões entregues; retenção; certificados de eliminação; lições e aprovação de encerramento.

Anexo J. Fontes autorizadas e data de verificação

35. Constituição de Moçambique, consolidação indicada pela WIPO Lex: WIPO Lex.
36. Lei n.º 3/2017, registo oficial: Imprensa Nacional; enquadramento do regulador: INTIC.
37. Lei n.º 13/2026 e Lei n.º 14/2026: Boletim da República, 1 de Julho de 2026.
38. Estado da proposta de protecção de dados: INTIC, 17 de Junho de 2026.
39. Sistema Estatístico Nacional e autorização: INE e procedimento de aprovação técnica.
40. Lei n.º 6/2023 e Decreto n.º 53/2024: Imprensa Nacional, Lei e Imprensa Nacional, Regulamento.
41. Convenção da UA: ratificação nacional e entrada em vigor reportada pela UA.
42. RGPD, texto oficial.
43. Manual do CICV sobre Protecção de Dados na Acção Humanitária.
44. Orientação Operacional do IASC sobre Responsabilidade de Dados.
45. OCHA Data Responsibility Guidelines.
46. OMS, Putting Women First e recomendações para investigação de intervenção.
47. UNEG Ethical Guidelines for Evaluation.
48. UNICEF Policy on Ethics in Evidence Activities, 2026.

PART II. ENGLISH GUIDELINES

1. Status, purpose and use

These Internal Guidelines on Ethical Data Collection and Data Governance set Data4Moz's minimum requirements for planning, collecting, transferring, processing, analysing, sharing, retaining and destroying data obtained from people, households, communities, institutions and geographic spaces. They apply to employees, consultants, subcontractors and partners acting for Data4Moz.

The document serves two purposes. It is an operating manual for field and data teams, and an auditable statement of the commitments Data4Moz makes to participants, clients, authorities and funders. A contract, deadline or client request does not permit a team to reduce these safeguards. Where law, ethics approval or contract requires a stronger safeguard, the stronger requirement applies.

STOP RULE: No collection starts without an approved protocol, defined purpose, tested instruments, clear contractual roles, confirmed legal basis, appropriate consent and safeguards proportionate to risk.

1.1 Assumptions used in this version

49. National coverage across urban, rural, remote, coastal and emergency- or conflict-affected areas of Mozambique.
50. Digital collection mainly through KoboToolbox/ODK and ArcGIS Survey123/Field Maps, with paper forms when needed.
51. Household and socioeconomic data; health and nutrition; children and adolescents; protection and gender-based violence (GBV); agriculture, livelihoods and natural resources; GPS, photographs, audio, video, imagery and drones.
52. Multiple clients and funders. Each donor's requirements are extracted from the contract and attached to the Project Data Responsibility Plan.
53. Data4Moz may be a controller, a processor for a client, or both at different stages. The contract must allocate each role before platforms are configured.

1.2 Approval and review

The document takes effect when approved by Data4Moz management. It must be reviewed at least annually and whenever a relevant law changes, a new data type or platform is introduced, a serious incident occurs, or a funder changes its requirements. Approval fields, complaint contacts and security roles must be completed before formal adoption.

LEGAL NOTE: This policy translates operational requirements and sources verified through 16 August 2026. It is not a substitute for legal advice. Before adoption, and for every high-risk project, Data4Moz must obtain confirmation from qualified Mozambican counsel on current instruments, regulations, permits and sector obligations.

2. Scope, terms and data classification

2.1 Activities covered

These rules cover interviews, focus groups, observation, anthropometry, administrative records, beneficiary lists, audits, monitoring and evaluation, community censuses, surveys, participatory mapping, asset tracking, telemetry, satellite or drone imagery, photographs, recordings, client-provided data, and data derived through analysis or artificial intelligence.

Metadata are also covered. Date, time, device identifier, GPS trail, interview duration, enumerator name and edit history can identify a person or expose a location and must be protected.

2.2 Operational definitions

54. **Personal data:** information that directly or indirectly identifies, or could reasonably identify, a person.
55. **Sensitive data:** data whose disclosure or misuse could cause discrimination, stigma, violence, loss of benefits, sanction, economic harm or a serious invasion of privacy. Examples include health, disability, HIV, GBV, protection, sexual life, children, biometrics, political opinion, religion, party or union affiliation, migration status, land conflict and vulnerable-person locations.
56. **Personal geospatial data:** coordinates, polygons, routes, images or spatial attributes linked to an identifiable person, household, plot, structure or activity.
57. **Anonymisation:** transformation that reasonably and durably prevents reidentification, taking account of other available data. Pseudonymised data are not anonymous.
58. **Pseudonymisation:** replacing identifiers with a code while retaining a separate key that enables reidentification.
59. **Controller:** entity that determines why and how data are processed.
60. **Processor:** entity processing data under the controller's documented instructions. Local legal terminology may differ; contracts must map roles and receive legal review.
61. **Participant/respondent:** a person who supplies data or about whom data are collected.

2.3 Classification levels

Level	Examples	Minimum rule
Public	Approved aggregate indicators, published methods, maps without reidentification risk	Authorised release and disclosure review
Internal	Training materials, schedules, blank forms	Access limited to authorised personnel and partners
Confidential	Pseudonymised microdata, business data, separate contact files, unpublished findings	Role-based access, encryption and controlled sharing
Restricted	Names linked to health/GBV/children, household GPS, biometrics, recognisable recordings, linkage keys, protection cases	High-risk approval, named access, access logging, stronger encryption and short retention

If uncertain, use the higher classification until the Data Manager and Data Governance Lead decide.

3. Core principles

3.1 Do no harm

Collection is justified only when the expected information benefit outweighs foreseeable risk. Teams assess physical, psychological, social, economic, legal, digital and reputational harm, including reidentification and the visible presence of a field team. A technically correct interview must stop if it exposes a respondent to violence, stigma, retaliation or loss of assistance.

3.2 Necessity, proportionality and minimisation

Collect only what is necessary for a defined question and decision. Every sensitive variable needs written justification. “It may be useful later” is not sufficient. If district, age band or a random code will serve the purpose, do not collect an address, exact birth date or name.

3.3 Purpose limitation

Before contact, Data4Moz defines purpose, users, outputs, retention and sharing. A new purpose requires a compatibility assessment, contractual and ethics authorisation and, where necessary, renewed consent. Monitoring data may not quietly become research, marketing, surveillance, eligibility screening or law-enforcement data.

3.4 Accuracy and integrity

Data4Moz must distinguish what was reported, observed, verified and inferred. Do not guess answers, alter data to meet targets or present self-report as verification. Corrections retain an audit trail. Accuracy protects participants from bad decisions and clients from indefensible findings.

3.5 Transparency

Participants must know who is collecting, for whom, why, what happens to the data, what risks exist and how to complain. Do not use vague descriptions to conceal sensitive topics. Explain real limits of confidentiality, such as a confirmed duty concerning imminent harm, before the interview.

3.6 Justice and inclusion

Do not exclude people because of language, disability, location, gender or poverty for team convenience. Do not place the burden of repeated studies on easy-to-reach communities. Reasonable adaptations must enable safe participation without lowering the standard of consent.

3.7 Demonstrable accountability

Compliance must be evidenced. Retain proof that risks were assessed, personnel trained, consent obtained, access controlled, complaints handled and data destroyed on schedule.

4. Mandatory pre-field gate

The Project Manager may not authorise mobilisation until the Project Compliance File contains:

62. contract and allocation of controller/processor roles, ownership, sharing, return and deletion;
63. objective, method, population, sample, inclusion criteria and substitution rules;
64. variable inventory, classification, data flow and server location;
65. Ethical and Data Protection Impact Assessment for any high-risk processing;
66. INE authorisation where applicable;
67. technical-scientific approval, ethics review, registration and health authorisations where applicable;
68. relevant administrative, community and aviation/drone approvals;
69. approved instruments, translations, consent scripts and referral plan;
70. secure platform configuration, accounts, roles, encryption, backup and restoration test;
71. retention, sharing, anonymisation and destruction plan;
72. complaint mechanism and contact materials in suitable languages;
73. training, assessment and certification for every team member;
74. pilot covering duration, privacy, comprehension, risk and technical function;
75. physical security, communication and evacuation plan for the work area.

DO NOT AUTHORISE: If a client requests identifiable data without a documented purpose, legal basis, security, time limit and data-sharing arrangement, suspend configuration and refer the request to management and the Data Governance Lead.

5. Community entry and cultural sensitivity in Mozambique

5.1 Respectful entry

Teams must use appropriate administrative and community channels. Depending on the location, this may include provincial or district authorities, administrative posts, localities, municipalities, bairro secretaries, régulos, traditional leaders, religious leaders or community committees.

1. Present a credential letter and explain the project, commissioning entity, locations, schedule, selection method, duration and complaint contact.
2. Ask about language, timing, safety, community events and visiting norms.
3. Explain that leaders facilitate entry but do not answer for households, see questionnaires or consent for individuals.
4. Ask leaders not to accompany interviews or pressure people to participate.
5. Record the entry meeting and agreed conditions without unnecessary political information.

Do: recognise legitimate local authority, provide advance notice and correct rumours. **Do not:** promise projects, payments or benefits; ask a régulo for a list of “good households”; accept one leader's account as the community response; display beneficiary lists.

5.2 Language and translation

Portuguese must not be presumed to be the preferred language. Prepare a site language map that may include Emakhuwa, Xichangana, Cisena, Elomwe, Echuwabo, Cinyanja, Ciyao, Shimakonde, Kimwani, Cindau and other local varieties. Do not treat a province as linguistically uniform.

6. Use a competent translator and an independent local reviewer for scripts and key terms.
7. Back-translate or use panel review, followed by cognitive testing with people similar to the target population.
8. Maintain an approved glossary for consent, health, nutrition, GBV, land tenure and response scales.
9. Do not improvise sensitive wording. If a concept has no direct equivalent, use an approved explanation and record the version.
10. Do not use children, neighbours, leaders or relatives as interpreters for sensitive topics. Professional interpreters sign confidentiality undertakings.
11. Record interview language and comprehension difficulties to assess bias.

5.3 Gender, age and power

For sexual health, GBV, protection, personal income or family relations, offer an interviewer of the respondent's preferred gender where feasible. An adult woman does not require her husband's permission to consent. The team must still assess retaliation risk and must not insist on an interview without privacy.

Do not assume the household head knows everyone's experience. Interview the selected person. Proxy interviews are allowed only under the protocol and must be marked as proxy. For children and adolescents, use guardian permission and assent, suitable privacy and the safeguarding plan.

5.4 Timing and household conduct

Schedule around work, school, market, farming, fishing, water collection, worship, meals, funerals, ceremonies and rest. Do not interview at night unless there is documented need, a safety plan and

a participant request. Ask before entering, sitting, photographing or touching property. Seek a place where others cannot hear. Use neutral tone, suitable dress and respectful distance. Do not comment on the home, religious practice, family relations or responses. Do not accept money. Approved compensation must be explained consistently and must not depend on answers.

5.5 Respecting norms without compromising integrity

Cultural respect does not permit fabrication, informal sample replacement, exclusion of women or youth, disclosure of answers or omission of consent. If a norm conflicts with safety, rights or method, the enumerator pauses, protects the participant and calls the supervisor. Document every approved adaptation.

6. Selection, contact and field quality

6.1 Recruitment

12. Use only authorised lists transferred securely.
13. Give mobilisers only what they need to locate a unit, never earlier answers or sensitive attributes.
14. Do not allow leaders, service providers or employers to observe who accepts or refuses.
15. Explain selection without implying that participation affects benefits.
16. Do not replace an absent or refusing household with a neighbour. Follow approved revisit and replacement rules with supervisor authorisation.
17. Obtain separate consent for follow-up contact or back-checking.

6.2 During the interview

Read questions as approved, probe neutrally, accept “do not know” and “prefer not to answer,” and separate observation from reported response. Do not suggest an answer, complete missing answers or copy a prior interview. Stop when:

18. the participant withdraws or cannot demonstrate understanding;
19. privacy is unavailable for a sensitive topic;
20. another person arrives and creates risk;
21. the participant is distressed, intoxicated, seriously ill or threatened;
22. a child refuses despite adult permission;
23. the device, form or selection is wrong;
24. someone demands access to answers;
25. there is physical danger to the participant or team.

6.3 Ethical quality control

Supervisors may use duration, routes, response patterns and authorised back-checks to identify error. These indicators do not prove fraud by themselves. Confirmation must be fair, confidential and documented. Audio audits, silent photographs or continuous tracking for quality control require notice, necessity and suitable consent; they are not enabled by default.

7. Informed consent

7.1 Conditions for valid consent

Consent is a process, not a signature. It must be informed, specifically, understood, voluntary and given by a person with capacity. It occurs before collection and remains valid throughout the activity. Participants receive, in understandable language and format:

26. identity of Data4Moz, the client and contacts;
27. purpose and reason for selection;
28. activities, duration and topics;

29. risks, discomfort and benefits, including no direct benefit;
30. compensation or reimbursement, if any;
31. data collected, uses, recipients, country/server where relevant and retention;
32. confidentiality protections and limits;
33. optional elements such as recording, photography, GPS and future contact;
34. right to skip, refuse or withdraw without penalty or loss of benefits;
35. how to request access, correction, withdrawal where possible, or complain.

Use teach-back: “Can you tell me in your own words what happens if you decide not to take part?”
Re-explain any misunderstanding. Do not turn teach-back into a test or embarrass the person.

7.2 Refusal and withdrawal

A refusal ends the contact respectfully. Do not ask why unless an optional approved item permits it. Do not send a leader, beneficiary or another enumerator to persuade the person. On withdrawal, stop and ask whether already collected data may be retained. Explain in advance that data already irreversibly anonymised may no longer be retrievable.

7.3 Limited literacy and oral consent

Read the full text, allow questions and document oral consent. If a witness is required, the witness should be an adult independent of the team and preferably not a leader, benefit provider or person with power over the participant. The record includes script version, date/time, participant code, language, enumerator code, oral method, teach-back result and witness code. A fingerprint is collected only if required and approved. It is a biometric identifier and is not the default answer to limited literacy.

7.4 Children and reduced capacity

For anyone under 18, Data4Moz's default is parent/legal guardian consent and age-appropriate child assent. The child's refusal prevails. Exceptions for emancipated minors, confidential adolescent services or unavailable guardians require documented legal and ethics approval. Do not interview a child in front of someone likely to influence answers, while following approved supervision and safeguarding. Do not promise absolute secrecy if the protocol requires action for immediate risk of harm. Explain that limit simply before asking.

Do not assume an adult lacks capacity because of disability, age, schooling or language. Provide communication support and follow the protocol's capacity assessment. A lawful representative and the person's assent are needed when capacity is genuinely impaired.

7.5 Separate permissions

Participation, photography, video, audio, attributed quotation, exact GPS, drone imagery, future contact and public use are separate decisions. A pre-ticked box or one “accept all” option is not specific consent. If GPS is essential, say that refusal prevents the activity but has no effect on benefits; do not claim that the person can continue when that is untrue.

8. Health, nutrition, GBV, protection and other high-risk topics

8.1 Mandatory screening

Require an Ethical and Data Protection Impact Assessment, specialist review and external ethics approval where applicable for individual health, children, GBV, violence, exploitation, trafficking, HIV, mental health, disability, biometrics, biological samples, illegal activity, land conflict, displaced people, refugees, minorities, threatened-species locations or any credible adverse consequence.

8.2 Health and nutrition

Human health research may be governed by Law 6/2023 and Decree 53/2024. Calling an activity “M&E” does not remove obligations if it constitutes human health research. Obtain a written determination from the client, INS/CNBS or counsel when uncertain. Anthropometry requires calibrated equipment, hygiene, privacy, specific consent, an approved clothing/contact procedure and practical training. Enumerators do not diagnose or promise treatment. Communicate clinically relevant findings only under a validated protocol with realistic referral and no false assurance of service.

8.3 Gender-based violence and protection

Collect violence data only when necessary, teams have specialist training, privacy can be assured and verified safety/referral procedures exist. Apply WHO recommendations that place participant safety first.

36. Use neutral study names and materials.
37. Interview only one eligible person per household when the protocol requires it.
38. Do not interview with a partner, relative, leader or child present.
39. Prepare a rapid switch to a neutral topic if someone approaches.
40. Do not store a name, number and violence narrative in the same file.
41. Do not include exact location in case reports or send cases by WhatsApp.
42. Do not confront alleged perpetrators or investigate beyond mandate.
43. Offer support information discreetly and only for verified services.
44. Explain reporting duties confirmed by law. Do not invent a duty or promise that no report will ever be made.

If privacy is unavailable, cancel or reschedule. Sample targets do not justify exposure.

8.4 Children and safeguarding

Every child project has a safeguarding focal point, code of conduct, contact rules, reporting channels and service map. No staff member remains alone with a child in an isolated place. Do not collect traumatic stories merely to illustrate a report. A child's identity, school, image and protection-case location are restricted data.

8.5 Agriculture, land, livelihoods and conservation

Tenure, plot boundaries, water access, income, informal practices, natural resources and disputes may affect rights or enforcement. Do not promise that mapping grants title, resolves a dispute or guarantees aid. Participatory maps must preserve disagreement and source, not convert the most powerful person's view into “community truth.” Sacred sites, resource routes, rare resources and threatened species must not be published at harmful precision.

9. GPS, photography, audio, video, imagery and drones

9.1 GPS

Before enabling location, define need, minimum accuracy, duration, access and output. Prefer a centroid, administrative unit, grid or displaced point when an exact address is unnecessary.

45. Explain that a coordinate may reveal a home, plot, workplace or route.
46. Keep the code-coordinate link in a separate restricted file.
47. Disable unnecessary continuous tracking, location history and metadata.
48. Do not publish household points. Aggregate, generalise or displace and test against roads, imagery and public lists.
49. Never invent an office coordinate for a refused or invalid point.

9.2 Photography, audio and video

Obtain separate permission for internal evidence, analysis/transcription, restricted client reporting, training and public communications. A person should be able to participate without appearing in a photograph unless imagery is the activity itself and was explained before selection.

Do not photograph forms, cards, screens, children, patients, survivors, homes or property without permission. Remove geotags when unnecessary. Store in an approved application, not a personal gallery or automatic personal cloud backup. A recognisable face or voice remains personal without a name.

9.3 Drones and aerial imagery

No flight occurs without written confirmation of current requirements from Mozambique's civil aviation authority, airspace and local permissions, qualified operators, insurance and safety assessment. Confirm the current instrument; this edition does not assert an RPAS directive number that could not be verified in an accessible official source.

Flight permission does not settle privacy. Notify the community of area, time, purpose, sensors and contact; avoid people, courtyards and private activity; plan resolution and angle to reduce identification; mask faces, plates and properties where needed. Raw imagery is restricted until reviewed. Secondary use requires a new assessment.

10. Collection-medium procedures

10.1 KoboToolbox/ODK

50. Individual accounts, strong passwords and MFA were available.
51. Form-level encryption with an organisation-managed key for confidential/restricted data.
52. Minimum roles: enumerators submit; supervisors review their team; exports limited to the Data Manager.
53. Disable unnecessary editing, attachments, audit data, device identifiers and location.
54. Test skips, constraints, calculations, languages, repeats, offline mode and network-loss scenarios.
55. Sync only to approved servers; verify receipt before deleting local copies.
56. Do not put real identifiers in filenames, support tickets or messages.

10.2 ArcGIS Survey123 and Field Maps

57. Named accounts, private groups, MFA and least privilege.
58. Hosted feature layers, web maps and attachments private by default; no public links.
59. Limit editing, export, sharing and offline sync by role.
60. Separate identifiable from analytic layers; use hosted views with reduced fields.
61. Test offline areas, sync conflicts, accuracy and device deletion.
62. Do not publish field maps or dashboards before disclosure review.

10.3 Devices

Prefer organisation equipment. Require a supported OS, full-device encryption, a PIN of six or more digits, two-minute auto-lock, updates, remote locate/wipe and inventory. Prohibit shared accounts, root/jailbreak, unauthorised apps, screenshots and automatic personal photo backup. Never leave a device unattended, lend it to a participant or transport it without control. Report loss or suspected access immediately, even if encrypted.

10.4 Paper

63. Use code instead of a name on the questionnaire where possible; keep consent and linkage lists separate.
64. Number forms and record daily issues, return and page counts.
65. Transport in a closed case; store in a locked cabinet with recorded access.
66. Do not leave forms in homes, hotels, vehicles or local offices.
67. Digitise in a controlled setting with double verification; do not use a personal phone.
68. Log transfer and destruction. Use secure shredding or an approved method with a witness and certificate.

11. Use, sharing, retention and destruction

11.1 Use limitations

Use data only for the explained and documented purpose. Linking to new databases, profiling, AI, facial recognition, marketing, eligibility screening or publishing individual cases requires review. Client data do not become Data4Moz's general-purpose asset.

11.2 Sharing

By default, clients receive aggregates and deidentified microdata. Transfer identifiable data only, when necessary, contractually authorised, covered by consent or another valid legal basis, and governed by a data sharing/processing agreement. The agreement defines purpose, fields, roles, storage, security, users, international transfer, subprocessors, onward-use and reidentification prohibitions, incidents, audit, term and deletion evidence. No onward sharing without written permission.

Refer requests from police, courts or public authorities to management and counsel. Enumerators never hand over a device, list or response on their own. Verify authority, form and minimum lawful disclosure.

11.3 Secure transfer

Use an approved portal, SFTP, temporary-access repository or another encrypted channel. Do not use open email, WhatsApp, unencrypted USB or public links. Confirm the recipient through a separate channel, expired access, limit downloads and log delivery.

11.4 Default retention schedule

The project's valid approved schedule governs where more protective. Otherwise use these maximums and delete earlier when purpose ends:

Record	Recommended maximum	Final action
Contact/recruitment list	90 days after field validation	Logged deletion
Name-code key and exact GPS	90 days after QA/acceptance unless approved follow-up	Delete or isolate for authorised follow-up
Audio/video for transcription or QA	30 days after use, maximum 90 days	Secure deletion
Identifiable microdata	12 months after final acceptance	Anonymise or delete
Pseudonymised analytic microdata	24 months after closure	Anonymise or delete
Consent and approval evidence	Contract/ethics term; default 5 years with minimal data	Restricted archive then deletion
Restricted GBV/protection/child data	Approved term, normally shorter than general data	Delete under ethics approval
Validated digitised paper	Maximum 90 days except consent	Certified destruction

Truly anonymous data/indicators	According to institutional value and licence	Governed archive
---------------------------------	--	------------------

Do not automatically apply telecom traffic or criminal-evidence retention periods to survey records. Counsel confirms any specific duty.

11.5 Destruction

Cover active, offline, export, temporary and device copies. Backups follow a documented cycle and remain unavailable outside controlled restoration. Approved cryptographic erasure may be used for encrypted storage. Log date, dataset, method, operator and verifier. Obtain a client deletion certificate where the client must delete.

12. Anonymisation and responsible disclosure

1. Remove direct identifiers: names, phones, ID numbers, addresses, photographs, voices and platform identifiers.
2. Separate and protect the linkage key.
3. Treat indirect identifiers: exact age, dates, rare occupation, household structure, school, village, employer and unique events.
4. Review free text, attachments, filenames and metadata.
5. Reduce spatial precision through aggregation, grids, generalisation or boundary-respecting displacement; test against imagery, roads and public data.
6. Assess rare combinations and sensitive-attribute inference. Metrics such as k-anonymity are diagnostic, not guarantees.
7. Suppress small cells. Default: do not publish counts below 5; use 10 or further aggregation for children, GBV, rare health events or small locations unless a documented review approves otherwise.
8. Obtain independent disclosure review before delivery or release.

Do not label data “anonymous” if they retain reidentifiable codes, exact GPS or recognisable narratives. Synthetic data and displaced-point maps also need risk testing.

13. Privacy and security throughout the lifecycle

13.1 Transit and storage

Confidential/restricted data require encryption in transit and at rest. Document provider, hosting region, subprocessors, backups, recovery, administrative access and cross-border transfer. Access is named, role-based and approved by the data owner, reviewed during the project and removed the same day a person leaves the team.

13.2 Analysis

Use approved workspaces with minimised, pseudonymised data. Do not copy to personal computers, email, messaging apps or generative-AI services without assessment, agreement and authorisation. Number and justify exports, then delete them. Tables, quotations and maps undergo disclosure control.

13.3 Backup and continuity

Maintain risk-proportionate encrypted copies separate from the primary environment with restricted access. Test restoration and document results. A backup must not become an indefinite archive.

13.4 Credentials and support

Never share passwords. MFA is mandatory for export, administration or restricted-data accounts. Support cases use no real data unless through an approved channel and only the minimum needed. Revoke temporary tokens, keys and links after use.

14. Data incidents and breaches

14.1 Events to report

Lost/stolen devices or paper; wrong recipient; public link; compromised account; malware; improper access; screenshots; personal-cloud sync; disclosure during interview; identifiable map point; unauthorised destruction or alteration; missing file; or reasonable suspicion.

14.2 Immediate action

1. Protect people and stop exposure.
2. Report to the supervisor and incident channel immediately, ideally within the first hour. Do not wait for proof.
3. Disconnect or revoke access when safe, without destroying evidence or changing logs.
4. Record time, data, device, people, actions and possible affected persons.
5. Follow instructions for remote lock, evidence preservation, credential change and provider contact.
6. Do not contact participants, media, police or clients outside the response plan.

The Security Lead and Data Governance Lead conduct an initial assessment within 24 hours: type, volume, sensitivity, encryption, likely access, consequences, jurisdictions, contract and measures. The Project Manager informs the client/controller without undue delay and meets the contractual deadline. If GDPR applies, the controller, with legal advice, decides on supervisory-authority notification within 72 hours and communication to data subjects. Laws 13/2026 and 14/2026 and their regulations may require CSIRT notification; confirm commencement and deadlines. Then contain, recover, investigate root cause, support affected people, correct controls, document notification decisions and review lessons. Good-faith early reporting must not be punished.

15. Roles and responsibilities

Role	Core responsibilities
Management	Approve policy, appoint responsible roles, resource controls, accept residual risk and ensure legal review
Project Manager	Define purpose/roles, complete compliance gate, secure approvals, resource safeguards and stop unsafe work
Data Governance/Protection Lead	Impact assessment, consent/sharing review, records, rights/complaints and incident support
Information Security Lead/CSIRT	Configuration, access, cyber risk, monitoring, response, backup and Law 13/2026 readiness
Internal Security Auditor	Independently verify controls and corrective action; not merely audit their own work
Data Manager	Dictionary, classification, platform, quality, pseudonymisation, export, retention and deletion
Field Manager	Community entry, secure logistics, language/gender staffing, complaints and physical incidents
Supervisor	Observation, support, daily review, revisit/substitution approval, chain of custody and escalation
Enumerator/Interpreter	Consent, privacy, faithful administration, device/paper security, immediate reporting and respect
Analyst	Minimisation, approved environment, reproducible analysis, disclosure control and export deletion

Subcontractor/Partner	Same duties, written agreement, training, limited access and deletion evidence
------------------------------	--

No person alone approves of an exception that benefits their deadline or deliverables. High risk requires the Project Manager, Data Governance and relevant technical/sector lead; legal questions require counsel.

16. Training, supervision and conduct

Before access, each person completes general and project training, signs confidentiality and conduct commitments, and demonstrates competence by test and role-play. An 80% passing score is recommended, with retraining before another attempt. Required topics: ethics, consent, language, sampling, privacy, platforms, security, incidents, complaints, prevention of sexual exploitation and abuse, and safeguarding.

GBV, children, health, anthropometry, biometrics and drones require specialist modules and practice. General induction does not qualify a person for these tasks. Supervisors hold daily debriefs, check consent and deviations, observe only with permission, review metrics without exposing responses and record corrective action. Management performs project audits and compliance sampling. Fraud, coercion, intentional disclosure or retaliation may lead to immediate removal from fieldwork and fair disciplinary review.

17. Complaints, rights and remedy

Each participant receives a card or oral information with a project code and low-cost channels: phone/SMS, email, local contact and address. Provide a route outside the direct supervisor for complaints about the team. Complete before fieldwork:

7. Data4Moz phone/SMS: **Project based**
8. Email: admin@data4moz.com
9. Ethics/safeguarding focal role: **Project based**
10. Independent client/donor channel where applicable: **When applicable**

Accept anonymous and local-language complaints. Record only what is needed, acknowledge within two business days, triage risk, escalate safeguarding immediately and aim to resolve within 15 business days or communicate a revised date. Retaliation and benefit withdrawal are prohibited. Carefully verify access, correction and deletion requests so data are not disclosed to the wrong person. Where Data4Moz caused harm, consider correction, publication withdrawal, notice, support, cost restoration or other proportionate remedy without requiring an improper waiver of rights.

18. Legal and standards framework

18.1 Mozambique: confirmed instruments and verification points

Instrument/status at 16-08-2026	Operational relevance	Data4Moz action
Constitution, consolidated through Law 1/2018; arts. 41, 68, 71	Privacy, image, home/communication; restrictions on identifiable belief, religion, affiliation and private-life data; access/rectification	Individual entry/consent; mandatory legal review before Article 71 categories; access/correction process
Law 3/2017, Electronic Transactions; arts. 63-65	Prior purpose, accuracy, confidentiality, security, rights, unauthorised access/transfer prohibition and processor responsibility	Apply to electronic collection; appoint responsible role and publish contact/practice information
Resolution 5/2019 and AU Cyber Security and Personal Data	Mozambique ratified; Convention	Align principles and ask counsel about

Protection Convention	entered into force 8-06-2023	direct/domestic effect for each issue
Personal Data Protection Bill	Official 17-06-2026 update said it was under parliamentary review; no official enacted law located by cutoff	Do not cite the bill as law. Monitor Parliament/INM/INTIC and revise on enactment
Law 13/2026, Cybersecurity	Published 1 July with commencement 90 days later; private-sector policy, risk, training, responsible person, internal auditor, CSIRT and incident duties; details await regulation	Transition plan before commencement; counsel confirms date, scope and regulations; management makes formal appointments
Law 14/2026, Cybercrimes	Criminalises unauthorised access, interception and interference; also delayed commencement	Written authority, named accounts, evidence preservation and legal response
Law 7/96 and Decree 34/98, National Statistical System	Prior INE authorisation for surveys by state/local/public or public-interest entities; statistical secrecy for official statistics	Screen government/public-interest surveys; obtain INE authorisation/written position; do not claim official-statistics authority without mandate
Law 6/2023 and Decree 53/2024, Human Health Research	Scientific approval, ethics review, registration and INS/CNBS/accredited-committee regulation as applicable	Determine whether health/nutrition/M&E is research; obtain approvals before recruitment
Law 7/2008, Child Rights, and Convention on the Rights of the Child	Best interests, privacy, protection and participation; under 18 as default child definition	Guardian permission, assent, safeguarding and minimisation unless approved exception
Law 34/2014 and Decree 35/2015, Right to Information	May cover private public-interest/resource activities while protecting dignity/private life	Coordinate requests with client/counsel; do not release personal microdata as “public information”
RPAS/IACM requirements	Current exact instrument was not verified in an accessible official source during review	Confirm in writing with IACM for every campaign, plus privacy and local permissions

18.2 International and donor standards

GDPR applies when its territorial scope or a contractual obligation triggers it, not simply because a donor is European. Document the trigger. Where applicable, address principles/accountability (Art. 5), lawful basis and consent (Arts. 6-7), special categories (Art. 9), controller-processor contracts (Art. 28), security (Art. 32), breaches (Arts. 33-34), impact assessments (Art. 35) and international transfers (Chapter V).

Data4Moz uses recognised references including the ICRC Handbook on Data Protection in Humanitarian Action, third edition; IASC Operational Guidance on Data Responsibility, revised 2023; OCHA Data Responsibility Guidelines, updated January 2025; WHO ethics and safety guidance for violence research; UNEG Ethical Guidelines; and UNICEF policy/procedures for evidence activities involving people, including children.

For each donor, the Project Manager extracts ethics review, hosting/transfer, incident deadline, ownership, access, publication, archive, audit, safeguarding and deletion terms. Add them to the Project Data Responsibility Plan and training.

19. Monitoring, exceptions and closure

Compliance indicators include trained/certified personnel, projects with impact assessments, pre-field approvals, MFA coverage, incidents and response time, complaints and resolution, access removal, deletion and destruction certificates. Exceptions are written, time-limited, justified, risk-assessed, independently approved and supported by compensating controls. There is no exception to voluntariness, non-coercion, child safeguarding, prohibition of fabrication or incident reporting.

Closure requires device/paper reconciliation, sync validation, account revocation, client return, deidentification, temporary-file deletion, subcontractor confirmation, compliance-file archive, incident/complaint report and the next deletion date.

Annex A. Enumerator pocket card

Before departure

11. Credential, emergency and complaint contacts.
12. Charged, updated and locked device with the correct form.
13. Language, sample, route, privacy and referral reviewed.
14. No unnecessary data, personal copies or old forms.

At every contact

1. Introduce yourself and confirm the selected person.
2. Seek privacy and the right language.
3. Read consent, check understanding and record the decision.
4. Ask neutrally; accept skips and pauses.
5. Obtain separate GPS/media/future-contact decisions.
6. Review without speaking answers aloud.
7. Thank, provide contact and leave safely.

Stop and call the supervisor

No consent; no privacy; child refuses; distress; threat; leader demands answers; wrong form; unauthorised GPS/photo; missing device/paper; promised benefit; sample deviation.

Annex B. Adult oral-consent base script

“Good morning/afternoon. My name is **[name]** and I work with Data4Moz. We are conducting **[clear project name/description]** for **[client]**. The purpose is **[purpose]**. You were selected through **[simple method]**.

If you agree, I will ask about **[topics]**. It will take about **[time]**. **[Explain measurement, observation or record access.]** Some questions may be personal or uncomfortable. You may skip, pause or stop at any time. Participation is voluntary. Refusal will not change any service, job, assistance or benefit now or later.

We do not promise a direct benefit. **[Explain compensation/reimbursement or say none.]** We will store your data **[how/where in understandable terms]** and limit access to the authorised team. Results will be **[aggregated/deidentified]**. **[Explain real confidentiality limits.]** We will keep identifiable data until **[date/period]**, then delete or anonymise it. **[Explain sharing and country if relevant.]**

You may contact **[channel]** with questions, complaints or a data request. What questions do you have? Can you tell me in your own words what happens if you decide not to take part? **[Re-explain as needed.]** Do you agree to participate?”

Record: yes/no; date/time; code; script version; language; enumerator; written/oral method; witness if required; teach-back result.

Annex C. Child/adolescent assent base script

“Hello. My name is **[name]**. We are speaking with children/young people to understand **[simple explanation]**. If you want to join, I will **[activity]** for about **[time]**. This is not a test and there is no right answer. You can say no, skip any question or stop. Nobody will take away a service or benefit because of your decision. **[Explain privacy and safety limit.]** Your parent/guardian said we may invite you, but the decision is also yours. Do you have questions? Do you want to take part?”

If the child says no, remains fearful and silent, moves away or persistently resists, stop. Do not ask the guardian to persuade them.

Annex D. Additional GPS, recording and image permission

Optional GPS: “We would like to record the approximate location of this **[household/plot/asset]** for **[purpose]**. The coordinate may show where it is. We will not publish the exact point and access is limited. You can refuse this part and continue. Do you agree?”

Essential GPS: “Location is required for **[reason]**. If you do not agree, we cannot use this interview, but refusal will not affect services or benefits. Do you agree?”

Audio: “We would like to record audio for **[transcription/quality]**. Only **[roles]** will listen and it will be deleted by **[date]**. You may refuse and **[continue/not continue, as the protocol states]**. Do you agree?”

Image: Record separate choices for internal evidence; restricted client report; training; public communications; use of name; child image with assent. Do not treat one choice as permission for all.

Annex E. Impact-assessment screening

If any answer is “yes” or “uncertain,” complete a full assessment before fieldwork:

8. Children, reduced capacity, displaced people, survivors or aid dependency.
9. Health, HIV, GBV, protection, biometrics, illegal activity, politics/religion or intimate life.
10. Names linked to sensitive data, exact GPS, recognisable audio/video/drone imagery.
11. Benefit, employment, enforcement, sanction or referral decision.
12. Database linkage, AI, profiling, recognition or individual prediction.
13. International transfer, new vendor or third-party access.
14. Large scale, small location, rare population or conflict risk.
15. No verified referral service, privacy or complaint channel.
16. New purpose, open publication or long retention.

The full assessment documents necessity, affected people, flow, harm, likelihood, controls, residual risk, consultation, decision and owners.

Annex F. Sharing checklist

17. Recipient identity confirmed.
18. Compatible purpose and field-by-field necessity.
19. Controller/processor roles and legal basis documented.
20. Consent/approval covers sharing.
21. Minimisation/anonymisation completed and reviewed.
22. Signed agreement prohibits reidentification and onward transfer.
23. International transfer and vendor reviewed.
24. Encrypted channel, expiry and named access.
25. Retention, deletion and evidence defined.
26. Log sender, recipient, date and version.

Annex G. Incident record

Record: number; reporter; date/time; place/system; factual description; categories and volume; classification; encryption; affected people; likely exposure; immediate measures; contacts;

client/controller; jurisdictions; deadlines; notification decision; support; cause; corrective action; closure and approval. Do not copy unnecessary personal data into the incident record.

Annex H. Supervisor verification

27. Credentials and consent correct.
28. Suitable privacy, language and gender.
29. Sample/revisit/substitution follows rules.
30. No promise, coercion or leader presence.
31. Separate GPS, media and future-contact decisions.
32. Sync, paper and devices reconciled.
33. Errors, refusals, distress, complaints and incidents escalated.
34. Unneeded exports and access removed.

Annex I. Compliance and closure file

Include: contract/DPA; legal advice; INE authorisation; health/ethics approval; local/IACM permits; impact assessment; instruments/translations; pilot; training/tests; access matrix; configuration; consent evidence; custody; QA; incidents; complaints; sharing agreements; delivered versions; retention; deletion certificates; lessons and closure approval.

Annex J. Authoritative sources and verification date

35. Mozambique Constitution, consolidated version listed by [WIPO Lex](#).
36. Law 3/2017, official listing: [National Press](#); regulator context: [INTIC](#).
37. Laws 13/2026 and 14/2026: [Official Gazette, 1 July 2026](#).
38. Personal-data bill status: [INTIC, 17 June 2026](#).
39. National Statistical System and authorisation: [INE](#) and [technical approval procedure](#).
40. Law 6/2023 and Decree 53/2024: [National Press, Law](#) and [National Press, Regulation](#).
41. AU Convention: [national ratification](#) and [AU report of entry into force](#).
42. [GDPR official text](#).
43. [ICRC Handbook on Data Protection in Humanitarian Action](#).
44. [IASC Operational Guidance on Data Responsibility](#).
45. [OCHA Data Responsibility Guidelines](#).
46. [WHO Putting Women First](#) and [intervention-research recommendations](#).
47. [UNEG Ethical Guidelines for Evaluation](#).
48. [UNICEF Policy on Ethics in Evidence Activities, 2026](#).