Guia de
Boas Práticas

PROTEÇÃO DE DADOS PESSOAIS E SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DE REGISTOS PÚBLICOS E ACESSO À JUSTIÇA NA GUINÉ-BISSAU

Este manual foi elaborado no âmbito do projeto "Apoio ao Sistema Integrado de Identificação Nacional" com o apoio financeiro da Confederação Suiça e apoio técnico do PNUD.

UNITED NATIONS DEVELOPMENT PROGRAMME, GUINEA BISSAU COUNTRY OFFICE EDIFICIO DAS NACOES UNIDAS, BISSAU, GUINEA-BISSAU

www.undp.org

Principal Autor(a): Rômulo Goretti Villa Verde

Designer: Carolina Braga Alvares

Colaboradores(as) UNDP: Minhone Nancanha Seidi, Armel Yapi, Lucas Rocha

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

PEACEBUILDING FUND

Introdução

Este Guia objetiva indicar boas práticas para assegurar a privacidade, a proteção e a segurança de dados pessoais nas atividades de organizações governamentais e da sociedade civil que atuam na gestão de registos públicos e promoção do acesso à justiça na Guiné-Bissau.

Sumário

01. Princípios

Qualquer atividade realizada com dados pessoais deve obedecer a princípios fundamentais para a proteção da privacidade de seus titulares e para prevenir o uso indevido, desproporcional ou abusivo das informações. Destacam-se, ao menos, cinco princípios:

FINALIDADE E ADEQUAÇÃO

Dados pessoais devem ser recolhidos e utilizados apenas para finalidades legítimas, legais, específicas e determinadas. Os dados não devem ser utilizados de forma incompatível com estas finalidades, tampouco para fins ilícitos, discriminatórios ou abusivos.

NECESSIDADE

Devem ser tratados apenas os dados estritamente necessários, pertinentes e proporcionais para as finalidades pretendidas, com base em sua utilidade real e atual. Deve-se deixar de recolher, utilizar, armazenar ou compartilhar aqueles que sejam excessivos.

QUALIDADE

Deve-se adotar medidas para garantir a qualidade dos dados utilizados, assegurando que estejam claros, exatos, completos, atualizados e relevantes para o tratamento.

TRANSPARÊNCIA E LIVRE ACESSO

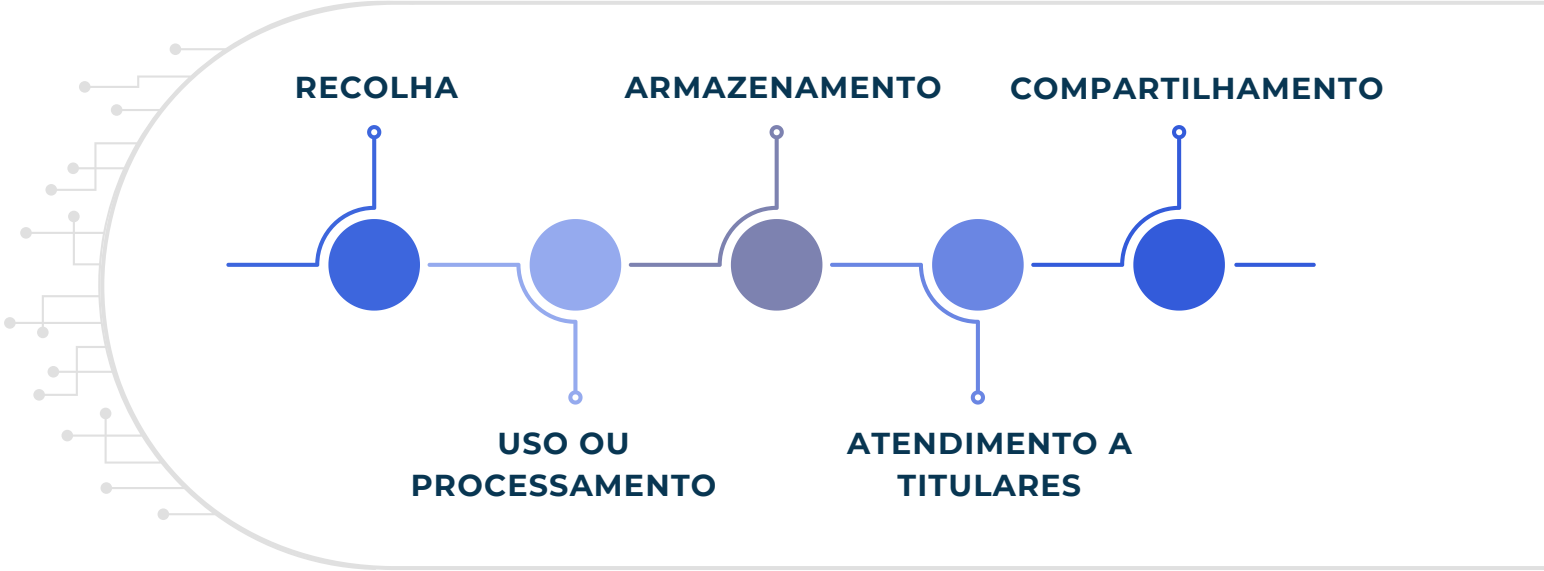
Os titulares devem receber informações claras, precisas e facilmente acessíveis sobre aspectos essenciais do tratamento, e devem possuir acesso facilitado a seus próprios dados pessoais.

SEGURANÇA E PREVENÇÃO

Devem ser adotadas medidas técnicas e administrativas para o sigilo e a segurança dos dados contra a exposição indevida, perda, destruição ou alteração não autorizada, e para a prevenção de danos aos titulares decorrentes do tratamento.

02. Boas Práticas

Para aplicar e operacionalizar os princípios do tratamento de dados pessoais (vide item 01), é necessária a adoção de medidas práticas. A seguir, serão indicadas boas práticas que podem ser adotadas em cada etapa do ciclo de vida dos dados em uma instituição.



Recolha

PEGUE APENAS O NECESSÁRIO

Solicite ou recolha apenas os dados efetivamente necessários para os propósitos específicos, legítimos, legais e previamente definidos de uso. Não recolha dados apenas porque “podem ser úteis, eventualmente”.

PLANEJE E PADRONIZE

Para evitar a recolha de dados excessivos, planeje e padronize os dados que serão solicitados para cada tipo de pessoa. Isso pode ser feito, por exemplo, pelo uso de documentos-padrão para preenchimento.

GARANTA A QUALIDADE

Assegure que os dados estejam claros, completos, atualizados e acurados. Isso pode ser feito pela conferência de documentos pessoais do titular, dos dados preenchidos em ficha, da confirmação oral de dados cadastrados etc. (conforme a necessidade e proporcionalidade na situação).

INFORME O TITULAR

Informe ao titular, ao menos, como os seus dados serão utilizados, e para quais propósitos. Se possível, e nos limites legais, informe também outras características essenciais do tratamento. Isso pode ser feito por informação verbal e/ou documento informativo facilmente acessível.

Recomenda-se informar:

- Como os dados serão utilizados, e para quê;
- Tempo de duração do tratamento;
- Com quais pessoas ou instituições os dados podem ser compartilhados, e para quais fins;
- Quais são os direitos do titular com relação aos seus dados, e como pode exercê-los.

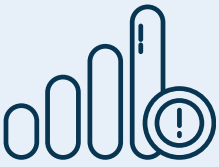
Uso ou Processamento

USE ADEQUADAMENTE

Utilize os dados pessoais de forma adequada e compatível com as finalidades específicas, definidas e informadas aos titulares. Não os utilize para propósitos desviantes dos originais, ou de forma desproporcional a eles.

CUIDE DOS RISCOS

Alguns tipos de dados, titulares e operações podem apresentar mais riscos que outros. Avalie se o uso dos dados traz riscos aos direitos e liberdades dos titulares, como:



- Risco de intrusão excessiva na privacidade e intimidade;
- Risco de uso de forma ilegal, discriminatória ou abusiva;
- Riscos à integridade física ou liberdade;
- Risco de prejudicar o acesso a serviços essenciais;

Adote medidas para reduzir ou afastar, na medida do possível e nos limites da lei, a probabilidade de que estes riscos ocorram.

Armazenamento

ARMAZENE COM SEGURANÇA

Opte por meios de armazenamento físicos e/ou digitais que preservem a disponibilidade dos dados, sua integridade e seu sigilo contra a exposição indevida e acesso não autorizado.

ARQUIVOS FÍSICOS

Para arquivos físicos, podem ser usadas salas reservadas da circulação do público, armários e gavetas com chaves. Deve-se proteger os documentos da luz, umidade, animais e de acessos de pessoas internas e externas não autorizadas.

ARQUIVOS DIGITAIS

Para armazenar arquivos digitais, recomenda-se a escolha de serviço ou sistema que ofereça:

- Armazenamento em nuvem e salvamento automático;
- Senha e controles de acessos;
- Controles de permissões para cada tipo de usuário;
- Histórico de versões e alterações;
- Outras garantias de segurança da informação. Ex: criptografia ponta-a-ponta para dados em trânsito e em armazenamento, certificado SSL...

PREVINA-SE CONTRA ATAQUES

Adote medidas técnicas e de conduta para prevenir-se contra ataques cibernéticos.

TECNOLOGIAS DE SEGURANÇA

Aplique tecnologias contra ataques cibernéticos nos computadores e dispositivos usados pela instituição. Exemplos: antivírus, antimalware, firewalls.

REDUZA VULNERABILIDADES

Reduza as vulnerabilidades dos dispositivos e sistemas, utilizando apenas programas de computador, aplicativos e sistemas operacionais originais. Além disso, mantenha-os sempre atualizados.

CONDUTAS DE SEGURANÇA

Evite clicar em links ou instalar arquivos executáveis de fonte suspeita ou desconhecida. Evite abrir e-mails ou mensagens sensacionalistas ou alarmistas. Utilize senhas fortes e seguras e jamais as compartilhe ou as deixe expostas.

CONTROLE OS ACESSOS

Estabeleça regras claras na instituição sobre quem pode acessar cada tipo de dado ou arquivo, em quais situações e para quais finalidades, de acordo com a necessidade do acesso para as atividades de cada cargo. Defina, ainda, a pessoa ou equipe responsável pela guarda dos dados.

Para arquivos físicos, implemente protocolos de controle e registo de retirada e devolução de documentos.

Para arquivos digitais, prefira serviços e sistemas de armazenamento com registo de acessos e atividades.

MANTENHA O BACKUP EM DIA

Faça sempre o backup de arquivos contendo dados pessoais, mantendo cópias atualizados em outro local, que pode ser:

- Virtual, como serviços de nuvem;
- Físico, como pendrives, HDs externos e servidores de dados.

DESCARTE OU ANONIMIZE

Reavalie periodicamente os dados armazenados, mantendo, em regra, apenas aqueles que continuem pertinentes e necessários. Proceda ao descarte seguro e definitivo dos dados excessivos, ou torne-os anônimos, eliminando as informações capazes de identificar o titular, nos limites da lei.

Atendimento a Titulares

ESCLAREÇA DÚVIDAS

Recomenda-se fornecer atendimento e esclarecimento gratuito e facilitado a dúvidas dos titulares relacionadas ao tratamento de seus dados pessoais. Por exemplo, dúvidas quanto às finalidades do tratamento, tempo de duração, mecanismos de segurança aplicados para a proteção, e informações sobre a existência de compartilhamento com terceiros.

OFEREÇA LIVRE ACESSO

Além das informações essenciais sobre o tratamento, recomenda-se permitir, sempre que possível e nos limites da lei, o acesso do titular aos dados pessoais que a instituição possui sobre ele. Isso pode ser feito pela entrega gratuita de um relatório ou cópia de seus dados. Lembre-se de verificar adequadamente a identidade do titular, para evitar fraudes.

GARANTA A QUALIDADE

Para garantir a qualidade das informações, deve-se permitir que os titulares corrijam, completem ou atualizem seus dados, se possível de forma gratuita e facilitada. No âmbito de registos públicos e de registos de trabalhadores do Governo, recomenda-se realizar iniciativas para promover novos registos e atualização dos já existentes.

Compartilhamento

COMPARTILHE O MÍNIMO

Restrinja o compartilhamento de dados com pessoas e instituições externas ao mínimo necessário. Para isso, defina as situações e os propósitos para os quais cada tipo de dado pode ser compartilhado com terceiros. O propósito do compartilhamento deve ser compatível com as finalidades originais de uso dos dados. Compartilhe apenas os dados estritamente necessários para estes propósitos.

Algumas formas de minimizar o compartilhamento de dados:

- Enviar apenas os dados solicitados, separadamente do arquivo original;
- Adicionar ao documento compartilhado elementos que escondam ou suprimam dados pessoais desnecessários;
- Compartilhar os dados de forma que não identifiquem o titular.

ATENÇÃO À SEGURANÇA

Adote medidas para garantir a segurança do compartilhamento, como:

Verifique a identidade do solicitante dos dados, quando cabível.

Esclareça ao destinatário dos dados os propósitos para os quais eles podem ser usados.

Implemente controle de entrada e saída de documentos e arquivos.

Use apenas meios seguros e institucionais para o compartilhamento.

DIVLUGUE COM CAUTELA

Na divulgação de informações pessoais de titulares ao público (como sites e mídias sociais), para fins jornalísticos e de promoção das atividades da instituição, é necessário ter cautela. Deve-se evitar a exposição excessiva e desproporcional dos titulares, especialmente quando estejam em situação de vulnerabilidade.

- Compartilhe apenas os dados necessários para atender ao interesse público da divulgação;
- Proteja a identidade da pessoa sempre que possível, evitando divulgar nomes e rostos;
- Evite a divulgação de imagens que possam expor a pessoa em momento de vulnerabilidade, ao desprezo ou perseguição, ou a situações vexatórias.

03. Gestão de Privacidade e Segurança

É importante definir e implementar procedimentos, rotinas e documentos para a gestão das práticas de proteção da privacidade e segurança da informação na instituição. Isso pode ser feito através de 03 passos essenciais (não necessariamente nesta ordem):

1°	Formalize regras internas, especificando as condutas que os colaboradores devem adotar com dados pessoais e segurança da informação.
2°	Defina responsabilidades de forma clara na instituição, para controle.
3°	Utilize instrumentos para esclarecer e atribuir obrigações de responsabilidade e sigilo.

1° PASSO - Regras internas

Estabeleça regras internas que formalizem as condutas esperadas dos colaboradores na instituição, quanto ao trato com dados pessoais e ao uso de dispositivos e equipamentos da instituição, com o objetivo de promover a privacidade e a segurança da informação.

As regras podem se dar no formato de Regulamento, Política, Código de Condutas, ou outros documentos equivalentes. Elas devem ser facilmente acessíveis a qualquer momento para consulta dos colaboradores.

O conteúdo das regras pode refletir as práticas recomendadas neste Guia. Ele também pode tomar por base os documentos referenciais elencados no Anexo I, assim como os direitos humanos e constitucionais, como a igualdade, as liberdades, a privacidade e a inviolabilidade da vida privada, a honra, a dignidade, o acesso à informação, dentre outros.

2º PASSO - Responsabilidades

Defina na instituição, de forma clara e expressa, as responsabilidades de cada colaborador com relação a procedimentos e documentos contendo dados pessoais. Por exemplo:

- Responsabilidade pela guarda de arquivos e controle de acessos;
- Responsabilidade pela fiscalização do cumprimento de regras internas;
- Responsabilidade pela autorização e registo de saída de dados da instituição;
- Responsabilidade pela análise e autorização de novas atividades com dados pessoais

3º PASSO - Instrumentos de obrigações

Utilize instrumentos escritos para estabelecer responsabilidades e obrigações com o uso e segurança de dados pessoais. Por exemplo:

- Termos de responsabilidade para colaboradores quanto ao uso ético e adequado de dados pessoais;
- Termos de sigilo e confidencialidade com dados pessoais;
- Termos de responsabilidade para terceiros, estabelecendo como os dados pessoais compartilhados pela instituição podem ser utilizados.

04. Glossário

Dados Pessoais

Qualquer informação relacionada a uma pessoa natural explicitamente identificada ou razoavelmente identificável, em meio físico ou digital. Ex.: nome, telefone, endereço, e-mail, profissão, cargo, foto, impressão digital, data de nascimento, naturalidade, eventos vitais, processos judiciais em nome da pessoa, situação socioeconômica etc.

Titular de Dados

A pessoa natural a quem os dados pessoais se referem.

Tratamento

Qualquer atividade realizada com dados pessoais, em meio físico ou virtual, de forma manual ou automatizada, como: acesso, recolha, registo, uso, processamento, análise, organização, catalogação, armazenamento, conservação, compartilhamento, envio, divulgação etc.

Anexo I - Bases Referenciais

Neste Anexo, indicam-se leis, tratados, convenções, diretrizes padrão internacionais, guias orientativos e normas técnicas que podem ser utilizadas como referenciais de base para a elaboração de regulamentos internos, políticas institucionais, novos projetos envolvendo dados pessoais, e normativos em privacidade, proteção de dados e segurança da informação na Guiné-Bissau.

Normas Gerais

Considerando-se que não há, ainda, lei ou regulamento específico na Guiné-Bissau sobre privacidade, proteção de dados ou segurança da informação, as leis guineenses relacionadas a registros públicos e à promoção do acesso à justiça podem ser utilizadas como bases referenciais gerais.

Assim, qualquer regulamento ou política internos, projeto com dados pessoais ou normativo no tema deve levar em consideração estas normas gerais pertinentes à atividade. Eles não podem estar em desacordo com estas leis, e devem, na medida possível, buscar garantir e aprimorar o seu cumprimento. São exemplos:

- Constituição da República da Guiné-Bissau;

  Especialmente o Título II, que trata dos direitos, liberdades, garantias e deveres fundamentais. Ele reconhece direitos importantes à privacidade e uso ético dos dados, como nos artigos 44, 51 e 52.

- Código Civil da Guiné-Bissau;

  Especialmente a Secção III, que trata dos direitos da personalidade. Ele reconhece direitos importantes à privacidade e uso ético dos dados, como nos artigos 70, 72, 79, 80 e 81.

- Decreto-Lei nº 6/2011 (Regulamento da Nacionalidade Guineense);
- Decreto-Lei nº 1/2011, (Plano Nacional de Registo Civil de Nascimento);
- Lei nº 11/2013 (Lei do Recenseamento Eleitoral);

Referenciais específicos

Na tabela abaixo, indicam-se bases referenciais pertinentes que trazem aspectos específicos em privacidade, proteção de dados pessoais e segurança da informação.

ESCOPO DE REFERÊNCIA	NOME	TIPO	LINK
Direitos Humanos	Declaração Universal dos Direitos Humanos (ONU)	Tratado	https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por
Direitos Humanos	Carta Africana dos Direitos Humanos e dos Povos	Tratado	https://www.dhnet.org.br/direitos/sip/africa/banjul.htm
Princípios (arts. 7º, 10º e 12º)	Lei nº 6/2007 (Lei de Bases do Sistema Estatístico Nacional)	Lei guineense	https://stat-guinebissau.com/Menu_principal/SEN/Legisla.html#:~:text=Lei%20n.%C2%BA%206%2F2007,t%C3%AAm%20verificado%20at%C3%A9%20ao%20presente.
Princípios	Declaração Africana sobre Direitos e Liberdades na Internet	Declaração	https://africaninternetrights.org/pt
Princípios e Framework regulatório	Suplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS	Tratado	https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf
Princípios e Estratégia regulatória (arts. 13 e 14 e Capítulo III)	Convenção da União Africana sobre Cibersegurança e Protecção de Dados Pessoais	Convenção	https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_p.pdf

ESCOPO DE REFERÊNCIA	NOME	TIPO	LINK
Implementação e operacionalização	Directrizes relativas à Protecção de Dados Pessoais para a África: Uma iniciativa conjunta da Internet Society e Comissão da União Africana	Guia orientativo	https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_201809June_Final_Portuguese.pdf
Princípios e Operacionalização	Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management (UN)	Guia orientativo	https://desapublications.un.org/publications/guidelines-legislative-framework-civil-registration-vital-statistics-and-identity
Framework regulatório	Regulamento Geral sobre a Proteção de Dados (UE)	Lei europeia	https://gdprinfo.eu/pt-pt
Framework regulatório	Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (Brasil)	Lei brasileira	https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
Framework regulatório	SADC Data Protection Model Law (HIPSSA Project, ITU)	Framework	https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf
Framework regulatório	Protection of Personal Information Act (África do Sul)	Lei sul--africana	https://popia.co.za/section-35-general-authorisation-concerning-personal-information-of-children/

ESCOPO DE REFERÊNCIA	NOME	TIPO	LINK
Estratégia de Governo Digital	Decreto nº 12.069/2024 - Estratégia Nacional de Governo Digital (Brasil)	Lei brasileira	https://www.planalto.gov.br/CCIVIL_03/_Ato2023-2026/2024/Decreto/D12069.htm#:~:text=DECRETO%20N%C2%BA%2012.069%2C%20DE%2021,per%C3%ADodo%20de%202024%20a%202027.
Desenvolvimento de sistemas	Guia de Digitalização de Registo Civil e Estatísticas Vitais (APAI - UNECA)	Guia orientativo	http://www.crvs-dgb.org/pt/
Desenvolvimento de sistemas	Practitioners Guide for Digital CRVS Systems (APAI - UNECA)	Guia orientativo	https://apai-crvs.uneca.org/sites/default/files/resourcefiles/practitioners_guide_for_digital_crvs_systems_171123.pdf
Framework operacional	ISO/IEC 27001:2022 (Information security management systems - Requirements)	Standard técnico	https://www.iso.org/standard/27001
Framework operacional	ISO/IEC 27002:2022 (Information security controls)	Standard técnico	https://www.iso.org/standard/75652.html
Framework operacional	ISO/IEC 27701:2019 (Privacy information management - Requirements and guidelines)	Standard técnico	https://www.iso.org/standard/71670.html
Framework operacional	ISO/IEC 24760:2019 (IT Security and Privacy - A framework for identity management)	Standard técnico	https://www.iso.org/standard/77582.html

ESCOPO DE REFERÊNCIA	NOME	TIPO	LINK
Framework operacional	ISO/IEC 29115:2013 (Entity authentication assurance framework)	Standard técnico	https://www.iso.org/standard/45138.html
Framework operacional	Digital Identity Standards (ENISA)	Guia orientativo	https://www.enisa.europa.eu/publications/digital-identity-standards
Framework operacional	NIST Cybersecurity Framework	Standard técnico	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
Framework operacional	NIST Privacy Framework	Standard técnico	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

Fontes de Orientação

As Autoridades de Proteção de Dados existentes no mundo são fonte constante de novos guias e orientações sobre temas específicos em privacidade, proteção de dados e segurança da informação. Abaixo, indicamos links pertinentes de algumas das principais Autoridades:

EDPB (UE)	https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pt
ICO (GB)	https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
AEPD (ES)	https://www.aepd.es/guias-y-herramientas/guias
CNIL (FR)	https://www.cnil.fr/en/decisions/lignes-directrices-recommandations-CNIL
ANPD (BR)	https://www.gov.br/anpd/pt-br/documentos-e-publicacoes
INFORMATION REGULATOR (ZA)	https://inforegulator.org.za/guidance-notes/
RAPDP (África)	https://www.rapdp.org/index.php/en/annuaire-des-membres


P N
U D