Entre em contato com o/a coordenador/a de Proteção de Dados pelo e-mail dpo@tearfund.org se tiver alguma dúvida.

Título:	**POLÍTICA DE PROTEÇÃO DE DADOS**
Declaração da política:	A Tearfund está comprometida em cumprir o Regulamento Geral de Proteção de Dados do Reino Unido ("RGPD do Reino Unido"), a Lei de Proteção de Dados de 2018 do Reino Unido (sigla em inglês: "DPA") e demais regulamentações aplicáveis em relação aos dados pessoais e a proteção dos direitos e das liberdades das pessoas cujas informações são coletadas e processadas pela Tearfund. Os procedimentos da Tearfund, de conformidade com o RGPD do Reino Unido e a DPA, são descritos nesta política, bem como nas políticas e nos procedimentos listados abaixo.
Procedimentos e outras políticas relacionadas com esta política	• Política de Retenção de Dados (em inglês) • Política de Segurança da Informação • Orientações sobre o Manuseio de Dados Pessoais (em inglês) • Aviso de Privacidade para os Funcionários • Política sobre Conduta Pessoal • Política de Denúncia de Irregularidades • Política de Coleta, Armazenamento e Uso de Conteúdos • Política Disciplinar • Guias do Usuário de Affinis • Uso de redes sociais em situações de alto risco aqui • Principais pontos a serem considerados ao compartilhar dados com a família Tearfund (em inglês) Todos os documentos acima estão disponíveis no Drive Compartilhado de Políticas da Tearfund, no Hub Corporativo, como apêndice desta política, ou no Hub Affinis, aqui, ou no Hub de Marca Global e Fotografia. • Termos de referência para o Grupo de Proteção de Dados • Relatórios de incidentes de violação de dados • Procedimento para solicitações de acesso de titular dos dados • Registro de atividades de tratamento de dados Os documentos acima estão disponíveis, mediante solicitação, através do/a cordenador/a de proteção de dados – dpo@tearfund.org. • Registros de armazenamento de dados Cada equipe tem seu próprio registro de armazenamento de dados e é responsável por mantê-lo atualizado.
Por que esta política é necessária:	O não cumprimento da legislação no tratamento de dados pessoais acarretará o risco de processo de execução e até mesmo ação judicial, além de pedidos de indenização por parte dos indivíduos. Há também questões de risco reputacional potencialmente sério.
Quem deve seguir esta política:	Todos na Tearfund, independentemente da localização ou função. Todos os empregados da família Tearfund, afiliados, voluntários, consultores ou representantes da Tearfund que precisem de acesso aos servidores e plataformas a fim de desempenharem suas funções.
Responsável:	Diretor/a financeiro/a reportando ao Conselho de Administração

Versão:	Final
Aprovada por:	CONSELHO DE ADMINISTRAÇÃO
Data de aprovação:	Julho de 2023
Próxima revisão formal:	Julho de 2025

Introdução

A proteção de dados refere-se à proteção do direito fundamental à privacidade, consagrado em leis e regulamentações. Todos os indivíduos precisam ter os meios para exercer seu direito à privacidade e proteger a si mesmos e às suas informações contra abuso. A Tearfund trabalha com um grande número de pessoas em todo o mundo e precisa coletar informações pessoais para executar seu trabalho. Todos os funcionários da Tearfund trabalham com dados pessoais como parte da função que exercem e, portanto, é essencial entender os princípios básicos de proteção de dados e as nossas responsabilidades.

Treinamento e recursos para proteção de dados

A Tearfund assumiu o compromisso de garantir que todos os funcionários entendam suas obrigações e responsabilidades relacionadas ao manuseio de dados pessoais. O curso on-line sobre Proteção de Dados é obrigatório para **todos** os funcionários, independentemente do seu local de trabalho na Tearfund. Se você tiver alguma dúvida sobre proteção de dados, envie um e-mail para: dpo@tearfund.org em primeiro lugar.

A Tearfund possui um/a coordenador/a de proteção de dados, bem como grupos dedicados a essa área, os quais são formados por representantes de toda a organização que se reúnem regularmente para revisar nossa conformidade com a proteção de dados.

O QUE SÃO DADOS PESSOAIS?

A política de proteção de dados aplica-se apenas ao tratamento de dados pessoais

- Os dados pessoais incluem apenas informações relativas a pessoas físicas que:
  - podem ser identificadas ou são identificáveis diretamente através das informações em questão;
  - podem ser indiretamente identificadas a partir da combinação dessas e outras informações.
- Os dados pessoais também podem incluir categorias especiais de dados pessoais ou dados de condenações criminais e delitos. Esses são considerados mais sensíveis e você só pode tratá-los em certas circunstâncias.

O QUE É TRATAMENTO?

- O RGPD do Reino Unido aplica-se:
  - ao tratamento de dados pessoais total ou parcialmente realizado através de meios automáticos; ou
  - outros tipos de tratamento de dados pessoais, não realizados através de meios automatizados, que fazem parte ou se destinam a fazer parte de um sistema de arquivamento.
- "Tratamento" é um termo muito amplo – ele inclui: coleta, manutenção, armazenamento e

compartilhamento.

O QUE SÃO DADOS PESSOAIS DA CATEGORIA ESPECIAL?

Dados pessoais da categoria especial (também chamados de sensíveis) são aqueles que revelam ou se relacionam com as seguintes características de um indivíduo:

- Origem racial ou étnica;
- Opinião política ou filiação sindical;
- Crenças religiosas ou filosóficas;
- Genética ou dados biométricos;
- Condições de saúde física ou mental;
- Vida sexual ou orientação sexual.

Para tratar dados da categoria especial, em geral, precisamos nos basear em um dos seguintes fundamentos:

1. Consentimento explícito do indivíduo;
2. Necessidade de cumprir com nossas obrigações e direitos na área de emprego e previdência social;
3. O tratamento de dados é necessário para alguns fins de saúde relacionada com o trabalho;
4. Exceção para ONG religiosa (tratamento realizado durante nossas atividades legítimas, com a proteção apropriada);
5. A informação relevante já foi comprovadamente tornada pública.

Com menos frequência, podemos nos basear nos seguintes fundamentos:

1. O tratamento é necessário em conexão com um processo judicial;
2. O tratamento é necessário para proteger os interesses vitais do indivíduo.

Se você precisar tratar dados de categorias especiais e não tiver certeza de que pode se basear em algum desses fundamentos, procure orientação junto à Equipe Jurídica da Tearfund.

- Os dados pseudonimizados podem ajudar a reduzir os riscos de privacidade, tornando mais difícil a identificação de indivíduos, embora ainda constituam dados pessoais.
- Se os dados pessoais puderem ser realmente anonimizados, eles não estarão sujeitos ao RGPD do Reino Unido. É importante entender o que são dados pessoais para entender se os dados foram anonimizados.
- As informações sobre uma pessoa falecida não constituem dados pessoais e, portanto, não estão sujeitas ao RGPD do Reino Unido.
- As informações sobre empresas ou autoridades públicas não constituem dados pessoais.
- No entanto, as informações sobre pessoas que atuam como microempreendedores individuais, funcionários, parceiros e diretores de empresas que são identificáveis individualmente, bem como as informações que se referem a eles como indivíduos, podem constituir dados pessoais.

PRINCÍPIOS DE PROTEÇÃO DE DADOS

Quais são eles? Por que os funcionários devem segui-los?

A Tearfund compromete-se a seguir os princípios do Artigo 5 do RGPD do Reino Unido e estabelece sete princípios fundamentais que se aplicam em todos os casos de tratamento de dados pessoais. A Tearfund mantém um registro contínuo de suas atividades de tratamento de dados pessoais, bem como do fundamento em que esse tratamento se baseia, em relação a cada atividade

Princípio 1: Os dados pessoais devem ser tratados de maneira lícita, leal e

transparente

De maneira lícita e leal: Precisamos ter fundamentos legais para tratar os dados pessoais, que possam ser entendidos pelo indivíduo. O tratamento dos dados pessoais deve seguir um dos seguintes fundamentos legais:

- Consentimento
  - *O **consentimento** precisa ser:*
    - ★ *dado através de um ato **claro e afirmativo** que estabeleça uma indicação **dada livremente, específica, informada** e **inequívoca** de que o titular dos dados concorda com o tratamento dos dados pessoais para um ou mais **objetivos específicos**.*
    - ★ *Precisamos ter provas do consentimento recebido se formos nos basear nisso.*
- Necessidade contratual
- Conformidade com as obrigações legais (por exemplo: divulgação de informações à Receita Federal do Reino Unido – HMRC)
- Interesses comerciais legítimos (por exemplo: verificações de antecedentes criminais)

Se você for se basear em interesses comerciais legítimos como fundamento jurídico para o tratamento de dados pessoais, você deverá primeiro preencher uma Avaliação de Interesses Comerciais Legítimos. O motivo disso é que os interesses comerciais legítimos da Tearfund devem ser ponderados face aos interesses ou direitos e liberdades fundamentais do indivíduo. O link para o modelo dessa avaliação encontra-se no Apêndice 1.

Com menos frequência, podemos nos basear em:

- Interesse público (prevenir ou detectar atos ilícitos)
- Interesses vitais

De maneira transparente: Precisamos comunicar aos titulares dos dados, em linguagem clara e simples, **como** usaremos seus dados pessoais no momento da **coleta.** Isso pode ser feito através de:

- Políticas de privacidade disponíveis em nosso site *www.tearfund.org*.
- Aviso de Privacidade para os Funcionários, cujo link está no Apêndice 1
- Redação expressa em formulários de consentimento impressos ou on-line (por exemplo: modelo de permissões de participantes, formulários de inscrição para eventos, formulários on-line, etc.)
- Explicações verbais – as quais devem ser gravadas
- Redação contratual

Avaliações de Impacto sobre a Privacidade de Dados *– uma avaliação de impacto sobre a privacidade de dados deve ser preenchida antes de qualquer tipo de tratamento de dados que possa acarretar um alto risco para os direitos e liberdades dos indivíduos. Essa avaliação deve ser preenchida quando houver um grande uso de dados sensíveis, dados relacionados a indivíduos vulneráveis ou tratamento que envolva um novo tipo de tecnologia. Um modelo de AIPD pode ser encontrado no Apêndice 1 e este deve ser aprovado pela Equipe Jurídica da Tearfund e pelo/a coordenador/a de Proteção de Dados da Tearfund. Uma vez que a AIPD tiver sido aprovada, os resultados poderão ser integrados no plano para o tratamento dos dados. A seguir, AIPD deverá ser revisada constantemente e reconsiderada sempre que necessário.*

Princípio 2: Limitação dos fins

Os dados pessoais só podem ser recolhidos para fins específicos, explícitos e legítimos e não podem ser posteriormente tratados de forma incompatível com esses

A Tearfund não deve obter informações para um fim e usá-las para outro. Devemos ser explícitos em relação ao uso dos dados pessoais.

Em mais detalhes:

A Tearfund identificou os seguintes "fins" para a nossa coleta de dados:

- *Administração:*
  - *Fins comerciais*
  - *Empregados (inclusive candidatos, voluntários, consultores e autônomos)*
  - *Apoiadores*
- *Correspondência de dados*
- *Marketing direto:*
  - *Apelos e atualizações de notícias*
  - *Campanhas*
  - *Eventos de captação de recursos*
  - *Captação de heranças*
  - *Eventos de voluntariado*
- *Pesquisa de mercado*
- *Criação de perfil*
- *Prospecção*
- *Prestação de serviços*

Se você estiver coletando dados pessoais para um fim que não acredita que se enquadre em uma das categorias acima, envie um e-mail para dpo@tearfund.org.

Exemplo:

Uma pessoa candidata-se a um emprego no site da Tearfund e fornece dados pessoais para fins de recrutamento (que se enquadram em administração: Empregados). O endereço de e-mail fornecido não deve ser usado, então, para enviar e-mails de marketing, a menos que tenhamos o consentimento expresso da pessoa para isso.

Princípio 3: Minimização de dados

Precisamos ser capazes de demonstrar que os dados pessoais são adequados, relevantes e limitados ao que é necessário relativamente às finalidades para as quais são tratados

Este é um exercício de ponderação entre coletar informações suficientes para o fim pretendido e, em paralelo, garantir que as informações não estejam sendo coletadas simplesmente "por via das dúvidas", caso sejam úteis. Esse princípio é relevante na elaboração de formulários do site ou pesquisas, por exemplo. Devemos considerar quais informações estamos coletando e por que precisamos delas. Também devemos ter cuidado ao registrar opiniões ou informações excessivas sobre indivíduos. Lembre-se de que o indivíduo pode pedir para ver as informações mantidas sobre ele/a e, assim, você terá que explicar por que as tem.

Exemplo:

Para fins de monitoramento e avaliação, a Tearfund pode coletar feedback de um grupo de participantes de um projeto para medir o impacto. Essa pesquisa pede informações da família, as quais constituem dados pessoais. No entanto, não há necessidade de que os participantes da pesquisa forneçam outras informações pessoais, tais como seu endereço. Portanto, essas informações adicionais não devem ser solicitadas. Isso garantiria que as informações coletadas sejam apenas as necessárias para o fim de medir o impacto. No entanto, se a Tearfund quisesse incluir um estudo de caso em que os participantes seriam identificados no relatório de impacto, precisaríamos do consentimento explícito dessas pessoas.

Princípio 4: Exatidão

Os dados pessoais devem ser exatos e, sempre que necessário, mantidos atualizados. Devem ser tomadas todas as medidas razoáveis para garantir que, levando-se em conta os fins do tratamento, os dados pessoais inexatos sejam excluídos ou retificados sem

demora

Sempre que possível, os funcionários devem usar fontes centrais para registrar e coletar dados (Affinis, SelectHR, IBIS etc.), pois elas devem estar atualizadas e corretas. Os funcionários não devem criar cópias desnecessárias Todo local que armazenar dados pessoais deve ser incluído no registro de armazenamento da equipe.

Os funcionários devem fazer as alterações necessárias nos dados assim que forem informadas ou quando forem percebidos erros. As informações desatualizadas devem ser destruídas.

Princípio 5: Limitação do armazenamento
Os dados pessoais não devem ser mantidos por mais tempo do que o necessário para os fins do tratamento
Precisamos garantir que possamos justificar a necessidade de continuarmos o tratamento (inclusive o armazenamento) de dados pessoais em formato eletrônico ou impresso.

Você deve garantir que os dados estejam sendo armazenados de acordo com os prazos estabelecidos na Política de Retenção de Dados (em inglês) e que você está familiarizado/a com as orientações sobre o manuseio de dados pessoais, ambos os documentos com links no Apêndice 1.

Em mais detalhes

- *Você deve nomear quaisquer documentos do Google que contiverem dados pessoais de forma que seja fácil saber (i) o que é documento; (ii) quando ele deve ser excluído; e (iii) limitar o acesso para que não haja várias cópias dos dados pessoais no Google Drive.*
- *Você deve excluir os dados pessoais da sua caixa de entrada de e-mails e de itens enviados assim que deixarem de ser necessários.*
- *Você deve se certificar de que o Registro de Armazenamento de Dados da sua equipe seja revisto trimestralmente e mantido atualizado – considere adicionar este item às reuniões regulares de equipe.*
- *Você deve saber como excluir e arquivar dados.*
- *Você deve excluir regularmente os itens da pasta "download".*
- *Anonimize as informações pessoais se quiser retê-las para fins estatísticos ou de pesquisa.*

Princípio 6: Integridade e confidencialidade (segurança)
Devem ser tomadas medidas técnicas e organizacionais apropriadas contra o tratamento não autorizado ou ilícito de dados pessoais e contra a sua perda, danos e destruição acidentais

Esta é potencialmente a maior fonte de risco para a Tearfund já que phishing e hacking representam um grande risco para todas as organizações internacionais. Todos os funcionários da Tearfund são responsáveis por garantir que os dados acessados permaneçam seguros e protegidos o tempo todo e devem garantir a conformidade com a "Política de Segurança da Informação", além de terem lido e entendido as "Orientações sobre Segurança Digital".

Em mais detalhes

A Tearfund emprega medidas organizacionais e técnicas. Por exemplo:

Organizacionais

1. *Treinamento sobre proteção de dados para funcionários*
2. *Política de Proteção de Dados e Política de Segurança da Informação*
3. *Orientações sobre Segurança Digital*
4. *Treinamento e orientação sobre o uso de documentos do Google*
5. *Disponibilização de armários trancados*

Técnicas

1. *Backups do sistema*
2. *Criptografia*
3. *Permissões de acesso a bancos de dados*
4. *Google Drive*
5. *Software de terceiros*

Cada um de nós tem um papel a desempenhar – desde trancar armários e bloquear computadores até não enviar emails para endereços incorretos ou dar acesso a informações pessoais a quem não precisa vê-las. Todos os funcionários devem estar familiarizados com a "Política de Segurança da Informação", que é divulgada anualmente e está disponível a qualquer momento no Hub Corporativo.

Princípio 7: Responsabilidade

O princípio da responsabilidade requer que a Tearfund assuma a responsabilidade pelos dados pessoais manuseados e sua conformidade com os outros seis princípios
É necessário ter sempre medidas e registros apropriados em vigor para demonstrar conformidade. A Tearfund fornece treinamento de integração obrigatório sobre proteção de dados, bem como revisão on-line obrigatória periódica para seus funcionários. O Grupo Principal de Proteção de Dados reúne-se regularmente para analisar as respostas para quaisquer violações de dados ocorridas e a conformidade da organização com as políticas e os procedimentos, e o Grupo Geral de Proteção de Dados, com representantes de todas as equipes da Tearfund, oferece mais uma oportunidade para a divulgação de lembretes sobre as melhores práticas.

A Tearfund nomeou um/a diretor/a de Proteção de Dados, que atua como ponto de contato com o Information Commissioner's Office (ICO - Gabinete do Comissário de Informação) e os titulares dos dados.

Outras questões importantes

Direitos de privacidade e proteção de dados dos indivíduos

A Tearfund respeita os direitos concedidos aos indivíduos pelas leis de proteção de dados, inclusive os direitos a:

- Acessar seus dados
- Restringir o uso de seus dados
- Corrigir a falta de exatidão de seus dados
- Excluir seus dados
- Restringir o contato não solicitado
- Ser notificados sobre violações de dados pessoais
- Ser informados sobre os critérios para qualquer tomada de decisão automatizada sobre si
- Reclamar

Para obter mais informações, envie um e-mail para dpo@tearfund.org.

Violações de dados pessoais

Em uma grande organização com atuação global, haverá ocasiões - que podem ser acidentais - em que os dados pessoais são excluídos, perdidos, alterados sem permissão ou divulgados ou acessados por indivíduos não autorizados a ver ou acessar as informações. Isso é definido como violação de dados pessoais. Ela engloba vários incidentes, tais como:

★ envio acidental dos dados de apoiadores para o endereço de e-mail errado;

- ★ perda em trânsito de modelos impressos de permissões de participantes;
- ★ roubo de laptop contendo dados pessoais;
- ★ notificação por parte de um fornecedor sobre o acesso ilegal a um de seus sistemas;
- ★ hacking do sistema ou da rede da Tearfund;
- ★ acesso incorreto dado a funcionários para um documento ou banco de dados contendo dados pessoais confidenciais.

A Tearfund possui um Plano de Resposta a Incidentes de Violação de Dados para responder às Violações de Dados Pessoais (e outras violações de segurança). A mensagem principal para todos os funcionários é que qualquer violação de dados de que você tomar conhecimento **deve ser relatada imediatamente** através de um e-mail para databreach@tearfund.org (*observação: se a violação envolver equipamentos de TI perdidos ou roubados, problemas de segurança ou qualquer outro tipo de incidente, você deve enviar um relatório de incidente para incident.reporting@tearfund.org, que, então, notificará databreach@tearfund.org sobre a violação de dados*). O motivo disso é que, se for necessário notificar o ICO, precisaremos fazê-lo sem atraso indevido e, se possível, no prazo de 72 horas a partir do momento em que tomarmos conhecimento da violação. Portanto, temos um prazo muito curto. Consulte o processo para notificar uma violação em mais detalhes.

Privacidade por design e por padrão

Antes de adotar um novo tratamento de dados ou realizar atividades que possam acarretar altos riscos à privacidade e aos dados pessoais, a Tearfund realiza e documenta uma avaliação de impacto de proteção de dados.

A Tearfund usa processos como a pseudonimização, para reduzir os riscos à privacidade dos titulares dos dados, ou a anonimização, para minimizar a coleta, o uso, o armazenamento ou qualquer outra forma de tratamento de dados pessoais.

Escopo do RGPD do Reino Unido

Como os escritórios nacionais da Tearfund não são entidades legais separadas e compartilham dados pessoais para os fins da Tearfund, aplicamos o RGPD do Reino Unido a esse tratamento em nosso trabalho. O RGPD do Reino Unido aplica-se, portanto, aos dados de participantes coletados no país, aos arquivos de RH dos funcionários do país etc. Esta é a razão por que todos devem seguir essa política.

Transferências internacionais

Qualquer acesso a informações pessoais em outro país será considerado como uma "transferência" para esse país. Por exemplo, se um funcionário abrir um documento do Google na Índia, que contenha dados pessoais, isso equivalerá a uma transferência desses dados para a Índia. De acordo com o RGPD, a posição padrão é que os dados pessoais não podem ser transferidos ou acessados fora do Reino Unido, a menos que uma ou mais das seguintes condições sejam atendidas: (i) a Comissão Europeia deve ter declarado que o país importador de dados é uma "jurisdição adequada"; ou (ii) devem ter sido implementadas salvaguardas apropriadas, como, por exemplo, Regras Corporativas Vinculantes ou Cláusulas Contratuais Padrão. O Reino Unido determinou que as leis de proteção de dados da UE são adequadas e a UE determinou que as leis de proteção de dados do Reino Unido são robustas o suficiente. Isso significa que os dados podem fluir com segurança do Reino Unido para a UE e vice-versa.

A Tearfund estabeleceu acordos de transferência de dados contendo cláusulas contratuais padrão para permitir a transferência de dados entre membros da família Tearfund, além de uma Declaração de Garantia ("Declaração") com relação à transferência de dados pessoais da Tearfund Reino Unido para outros escritórios nacionais da Tearfund.

Legislação local

Juntamente com esta política, as leis aplicáveis nos países onde a Tearfund opera devem ser seguidas durante a coleta e o tratamento de dados pessoais. Nos casos em que essas leis exigirem uma proteções mais rigorosas para os dados pessoais, a Tearfund deverá cumpri-las totalmente e implementar quaisquer políticas e processos adicionais que forem necessários.

Compartilhamento de dados pessoais

Os dados pessoais (inclusive informações básicas, tais como nomes) não devem ser compartilhados com terceiros fora da Tearfund (inclusive prestadores de serviços contratados, fornecedores, parceiros, doadores etc.), a menos que esse compartilhamento esteja em conformidade com os Princípios de Proteção de Dados e que haja um contrato em vigor, bem como a garantia (que deve estar no contrato) de que o terceiro possui medidas técnicas e organizacionais apropriadas para proteger os dados pessoais. A equipe jurídica da Tearfund possui cláusulas padrão de proteção de dados compatíveis com o RGPD para serem incluídas em seus contratos. Envie um e-mail a legal@tearfund.org para obter a cláusula padrão do RGPD da Tearfund.

Crianças e proteção de dados

Quando nos basearmos no consentimento como fundamento para o tratamento de dados pessoais de crianças, somente as crianças maiores de 13 anos podem consentir (no Reino Unido; em outras jurisdições da UE a idade pode ser 16 anos). Para as crianças menores de 13 anos, precisaremos do consentimento da pessoa com responsabilidade parental pela criança, devendo-se tomar medidas razoáveis para verificá-lo.

Apêndice 1

1. Aviso de Privacidade para os Funcionários
2. Avaliação de Interesses Comerciais Legítimos (em inglês)
3. Política de Retenção de Dados (em inglês)
4. Orientações sobre o Manuseio de Dados Pessoais (em inglês)
5. Avaliação de Impacto sobre a Privacidade de Dados (em inglês)