



Política de confidencialidade e proteção de dados

Atualizado em: julho de 2025	Próxima revisão: julho de 2027
Proprietária: Serviço pelos Direitos da Mulher Latino-americana (LAWRS)	
Autorizado por: Conselho Gestor de LAWRS	

Princípio: O Serviço pelos Direitos da Mulher Latino-americana (LAWRS) acredita firmemente que nossas usuárias têm direito a um serviço confidencial.

Objetivo: O objetivo desta política é definir os princípios aos quais a organização adere para garantir que as informações que nos são fornecidas sejam utilizadas de forma adequada e justa e permaneçam protegidas, construindo uma relação baseada na confiança. LAWRS usará essas informações apenas para o propósito para o qual foram coletadas.

Cobertura: A política se aplica a todos os aspectos da organização e a todas as pessoas das quais LAWRS coleta, processa e armazena informações pessoais, tais como, mas não limitado a , membras do Conselho Gestor, funcionárias , voluntárias, usuárias de serviços , membras e doadoras, freelancers, participantes de eventos, visitantes do prédio (individualmente e coletivamente).

Conteúdo:

1. Introdução
 2. Definições
 3. Princípios Gerais
 4. Armazenamento, acesso e gestão de dados
 5. Mídia
 6. Pesquisa
 7. Dados estatísticos
 8. E-mails, telefone e correio
 9. Exceções
 10. Sanções em caso de quebra de confidencialidade
 11. Procedimento de reclamações
 12. Lei de proteção de dados
 13. Registro de Atividades de Processamento (ROPA) e destruição de informações
 14. Avaliação do Impacto da Proteção de Dados (DPIA)
- Apêndice 1: Formulário de consentimento da usuária de serviços
Apêndice 2: Formulário de solicitação de dados pessoais
Apêndice 3: Formulário para informar quebra de confidencialidade
Apêndice 4: Orientações sobre o envio de e-mails em massa pelo Lamplight

Apêndice 5: Aviso de privacidade de LAWRS (para usuárias de serviços e público em geral)

Apêndice 6: Aviso de Privacidade de LAWRS para funcionárias e voluntárias

Apêndice 7: Avaliação de Impacto sobre a Proteção de Dados

1. Introdução

Os princípios descritos na política devem ser aplicados a todos os aspectos do trabalho de LAWRS.

LAWRS acredita que é necessário proteger todas as informações pessoais relativas às pessoas. Todas as informações pessoais devem ser coletadas, processadas e armazenadas de maneira legal, justa e transparente.

As informações pessoais coletadas por LAWRS devem ser precisas, relevantes e limitadas ao necessário em relação aos propósitos para as quais são processadas e não devem ser mantidas por mais tempo do que o necessário de acordo com o Registro de Atividades de Processamento (ROPA). LAWRS envidará todos os esforços para manter as informações seguras e precisas, de acordo com os procedimentos padrão.

Todas as funcionárias e voluntárias receberão uma cópia desta política durante o processo de integração e deverão participar de um treinamento básico sobre o GDPR e segurança na internet. Durante a integração, as voluntárias deverão assinar o acordo de voluntariado que contém uma seção sobre confidencialidade (consulte a Política e o Procedimento de Voluntariado de LAWRS). Além disso, as funcionárias e as voluntárias serão notificadas sempre que a política for atualizada.

2. Definições

Informações pessoais são os dados que identificam um indivíduo, que podem incluir dados confidenciais, como, mas não limitados a, nome, endereço, número de telefone, estado civil, orientação sexual e nacionalidade, número de filhos, status imigratório, origem étnica, candidaturas a empregos, avaliações, entre outros.

A proteção de informações pessoais se aplica a informações discutidas pessoalmente, virtualmente ou por telefone, que serão registradas nos sistemas de LAWRS de forma que permita identificar como os dados foram coletados. Podem ser armazenadas em cópia impressa, em computadores, em armazenamento em nuvem, em vídeo, como áudio ou em qualquer outra forma disponível e legal.

As administradoras de LAWRS são as Encarregadas pela Proteção de Dados (DPO) designadas e, como tal, são responsáveis por controlar e supervisionar as informações pessoais e fornecer aconselhamento para o gerenciamento de dados de novos projetos.

3. Princípios Gerais

3.1 Consentimento informado e base legal para o processamento

LAWRS processa dados pessoais de acordo com o RGPD do Reino Unido e a Lei de Proteção de Dados de 2018. Isso inclui informações pessoais básicas (por exemplo, nome, dados de contato) e dados de categorias especiais (por exemplo, saúde, etnia, status migratório), quando relevantes para nossos serviços.

LAWRS obterá o consentimento (verbal ou escrito) das pessoas antes de coletar quaisquer dados pessoais (ver Apêndice 1). LAWRS obterá o consentimento explícito das pessoas antes de processar dados de categorias especiais, exceto quando formos obrigados ou autorizados por lei a agir sem consentimento (por exemplo, em situações de proteção, risco grave à vida ou divulgações legais). O consentimento deve ser dado livremente, específico, informado e inequívoco. O consentimento pode ser escrito ou verbal e deve ser registrado no sistema de gerenciamento de casos Lamplight. Portanto, as pessoas devem ser informadas e compreender por que seus dados estão sendo coletados, como os dados serão usados, com quem podem ser compartilhados (se for o caso), por quanto tempo serão mantidos e seus direitos, incluindo como retirar o consentimento.

No momento da coleta de dados pessoais, LAWRS fornecerá à pessoa uma cópia de seu Aviso de Privacidade ou indicará claramente onde ele pode ser acessado (por exemplo, no site de LAWRS ou como uma cópia impressa na recepção). Se os dados pessoais forem obtidos de outra fonte, LAWRS fornecerá ao titular dos dados uma cópia de seu Aviso de Privacidade dentro de um período razoável de tempo (dentro de um mês).

Os funcionários e voluntários devem coletar apenas o mínimo necessário de dados pessoais e garantir que todas as entradas:

- Reflitam as necessidades da usuária
- Sejam informações factuais sobre o que foi discutido e as implicações relevantes para o caso
- Estejam livres de qualquer preconceito
- Sejam relevantes
- Sejam legíveis e registradas com precisão
- Sejam acompanhadas pelo nome da pessoa que as coletou e pela data

Todos os membros da equipe são responsáveis por controlar que LAWRS possua o consentimento necessário das pessoas, de acordo com a legislação aplicável, o que também deve ser documentado de forma adequada no sistema de gerenciamento de casos de LAWRS.

A LAWRS mantém um Registro de Atividades de Processamento (ROPA) que descreve a base legal e o período de retenção para cada atividade de processamento (ver Seção 13).

3.2 Compartilhamento de dados pessoais com terceiros

LAWRS não compartilhará informações pessoais sobre indivíduos com terceiros sem o seu consentimento expresso, com exceção de questões de segurança que exijam a divulgação aos Serviços Sociais ou à Polícia, em conformidade com a legislação aplicável e com a Política e os Procedimentos de Salvaguarda e Proteção Infantil de LAWRS, bem como com a Política e os Procedimentos de Salvaguarda e Proteção de adultos.

As funcionárias podem compartilhar informações com outros membros da equipe de LAWRS, desde que sejam relevantes para o caso (por exemplo, encaminhamento interno). Isso também se aplica às voluntárias quando estão auxiliando as funcionárias. Nesses casos, as funcionárias e voluntárias devem garantir que as informações pessoais não serão discutidas fora das instalações de LAWRS, a não ser que seja durante reuniões de supervisão externa. Da mesma forma, os arquivos contendo dados pessoais não devem ser removidos das instalações, a não ser que tenha sido concedida autorização adequada para tal pela usuária (por exemplo, para comparecer a audiências judiciais).

LAWRS pode entrar em contato com terceiros para o benefício da pessoa, tais como, mas não se limitando a, supervisor clínico, advogados ou qualquer outra organização, a fim de fornecer um serviço de alta qualidade. No entanto, isso só acontecerá com o consentimento expresso da pessoa, que deve ser devidamente informado.

Em conformidade com os requisitos do RGPD do Reino Unido, LAWRS utiliza um sistema digital seguro de gestão de casos denominado Lamplight, fornecido pela Lamplight Database Systems Ltd, para armazenar e gerenciamento dados pessoais. O Lamplight atua como processadora de dados em nome de LAWRS e não acessa nem compartilha dados pessoais, exceto quando necessário para manter e dar suporte ao sistema. Todo o processamento é regido por um Acordo Formal de Processamento de Dados, incluindo salvaguardas relativas ao acesso, hospedagem, criptografia e transferências internacionais de dados.

3.3 Direito de retirar o consentimento

As pessoas são livres para retirar seu consentimento a qualquer momento, mas isso pode impedir que LAWRS preste os serviços solicitados, no todo ou em parte. Os pedidos de retirada do consentimento (total ou parcial) podem ser feitos a qualquer membro da equipe, que deverá:

- Explicar os próximos passos e as possíveis implicações da retirada do consentimento à solicitante;
- Preencher e enviar o formulário de solicitação de dados pessoais (Apêndice 2) à sua gerente e à DPO por e-mail no mesmo dia da solicitação.

Uma vez recebido o formulário de solicitação, a DPO e a gerente relevante têm 7 dias úteis para consultar e avaliar os possíveis efeitos da retirada do consentimento para a prestação de serviços.

No prazo de oito dias úteis a partir da data da solicitação, a DPO informará (por e-mail, se possível) a usuária de serviços sobre as implicações de sua solicitação e solicitará sua confirmação para prosseguir com ela.

Levando em consideração a decisão da usuária e a avaliação das implicações, a DPO processará, executará qualquer ação relevante e registrará a solicitação no sistema de gerenciamento de casos de LAWRS.

LAWRS procurará resolver os pedidos no prazo de 8 dias úteis. Se isso não for possível, por qualquer motivo, deverá ser enviada uma atualização do andamento do processo à requerente, indicando quando poderá ser esperada uma resposta completa.

A seguinte declaração será exibida em inglês, espanhol e português de forma proeminente em nossos escritórios, na área de espera, em todos os momentos:

“LAWRS oferece um serviço confidencial. Nenhuma das informações compartilhadas conosco será divulgada a qualquer outra organização ou pessoa sem o seu consentimento expresso, a menos que exigido por lei ou pelas políticas de proteção de LAWRS”.

Você tem o direito de retirar seu consentimento a qualquer momento, no entanto, isso pode afetar a capacidade de LAWRS de prestar serviços.

Uma cópia da política de confidencialidade e proteção de dados de LAWRS está disponível mediante solicitação.

3.4 Direito ao esquecimento, também conhecido como Direito ao Pedido de Apagamento

As pessoas também têm o direito a serem esquecidas e LAWRS compromete-se a cumprir esse direito, a menos que existam obrigações legais ou quaisquer outros motivos razoáveis para manter os registros pessoais dentro dos prazos estabelecidos (ver ponto 13). Os pedidos de esquecimento podem ser feitos a qualquer membro da equipe, que deverá:

- Explicar os próximos passos e as possíveis implicações de ser esquecido à requerente;
- Preencher e enviar o formulário de solicitação de dados pessoais (Apêndice 2) à sua gerente e à DPO por e-mail no mesmo dia da solicitação.

Assim que o formulário de solicitação for recebido, a DPO entrará em contato com a gerente sênior relevante dentro de 2 dias úteis para confirmar se os dados pessoais da requerente podem ser excluídos de acordo com os acordos dos financiadores.

No prazo de 15 dias úteis a partir da data da solicitação, a gerente sênior relevante deve informar à DPO as conclusões dos detalhes dos acordos relevantes dos financiadores.

A DPO informará (por e-mail, se possível) ao solicitante quais dados serão apagados, quais dados serão mantidos e por quê.

A DPO então processará, executará qualquer ação relevante e registrará a solicitação no sistema de gerenciamento de casos de LAWRS.

LAWRS procurará resolver as solicitações no prazo de 20 dias úteis. Se isso não for possível, por qualquer motivo, uma atualização do andamento do processo deverá ser enviada ao solicitante, com uma indicação de quando uma resposta completa poderá ser esperada.

3.5 Solicitação de acesso do titular dos dados pessoais (SAR)

Nos termos do RGPD do Reino Unido, todas as pessoas têm o direito de acessar os dados pessoais que LAWRS detém sobre elas. As solicitações de acesso do titular dos dados (SAR) podem ser feitas verbalmente ou por escrito, e LAWRS deve responder no prazo de um mês civil após a recepção do pedido.

Se uma solicitação for particularmente complexa ou envolver um grande volume de dados, LAWRS poderá prorrogar o prazo de resposta por até dois meses adicionais. Nesses casos, a pessoa será informada da prorrogação e dos motivos para tal dentro do prazo original de um mês.

As solicitações podem ser enviadas a qualquer membro da equipe. Ao receber uma solicitação, a trabalhadora deverá:

- Explicar os próximos passos e prazos previstos ao solicitante
- Preencher e enviar o Formulário de Solicitação de Dados Pessoais (Apêndice 2) à sua gerente e à DPO no mesmo dia
- O seguinte procedimento interno deve ser seguido:
 - Dia 0–2: A DPO deve notificar a gerente sênior relevante
 - Dia 3–15: A gerente sênior deve reunir os dados solicitados e avaliar se a divulgação pode representar riscos para a pessoa (por exemplo, sofrimento emocional, complicações legais)
 - Dia 16–20: A DPO informa a solicitante sobre quaisquer riscos potenciais e confirma se ela deseja prosseguir
 - Dia 21–30: A DPO fornece os dados solicitados à pessoa (por escrito, de preferência por e-mail seguro) e registra a solicitação no sistema de gerenciamento de casos Lamplight.

Se a solicitação não puder ser concluída dentro de um mês civil, a DPO notificará a pessoa até o dia 30 com uma explicação e um prazo revisado, não excedendo dois meses adicionais.

Não será cobrada nenhuma taxa pelas SARs, a menos que a solicitação seja manifestamente infundada, excessiva ou repetitiva. Nesses casos, LAWRS poderá cobrar uma taxa razoável ou recusar a solicitação, de acordo com o Artigo 12(5) do RGPD do Reino Unido.

4. Armazenamento, acesso e gestão de dados

Os dados devem ser armazenados da seguinte forma:

- Todos os arquivos impressos contendo informações pessoais serão mantidos em armários trancados.
- Todos os dados eletrônicos serão armazenados em sistemas protegidos por senha, e as senhas serão alteradas quando necessário (por exemplo: mudança de pessoal, suspeita de vazamento).
- Cada membro da equipe terá um nome de usuário e senha pessoais para acessar a rede de LAWRS e o sistema de gerenciamento de casos Lamplight. As credenciais nunca devem ser compartilhadas.
- A autenticação de dois fatores será configurada para acessar e-mails, armazenamento em nuvem e o sistema Lamplight.
- As DPOs são responsáveis por monitorar a mudança de senhas.

4.1 Documentação de casos e registros de trabalho

LAWRS registra toda a documentação de casos e dados das usuárias de serviços principalmente no sistema de gerenciamento de casos Lamplight, que funciona como um repositório digital seguro para todas as interações com usuárias de serviços, notas complementares, documentos e encaminhamentos. Não são mantidos registros em papel, a menos que seja estritamente necessário por motivos legais ou processuais (por exemplo, processos judiciais). Quaisquer documentos físicos devem ser carregados de forma segura no Lamplight e destruídos imediatamente depois. Se um documento em papel precisar ser mantido por exigências legais, a equipe de gestão sênior é responsável por garantir que todos os documentos sejam mantidos trancados em armários de arquivo.

O sistema Lamplight é hospedado na Área Econômica Europeia (EEA) (EEE) pela Amazon Web Services (AWS) e é protegido por criptografia, controles de acesso baseados em funções, autenticação multifatorial e registro de auditoria. O acesso é restrito a funcionárias autorizadas e voluntárias supervisionadas, aos quais são atribuídas contas individuais com níveis de permissão definidos com base em suas funções.

Todos os registros de casos devem:

- ser inseridos no mesmo dia útil da sessão ou contato (quando possível)
- conter apenas informações factuais, relevantes e respeitadas
- ser atribuídos à funcionária ou voluntária que inseriu o registro

As voluntárias só podem acessar os registros das usuárias no Lamplight sob supervisão e para os casos aos quais foram formalmente designadas. Elas não devem manter cópias ou anotações fora do sistema.

Trabalho remoto e offline

Se uma consultora precisar trabalhar offline (por exemplo, em atividades externas sem acesso à Internet), as anotações devem ser feitas em um arquivo dedicado protegido por senha e carregadas no Lamplight dentro de 24 horas, após o que a cópia local deve ser eliminada.

Retenção e eliminação de dados

As DPOs monitoram os casos para a eliminação de dados anualmente para confirmar a ação ou estender a retenção quando houver uma retenção legal.

4.2 Uso de telefones celulares e aplicativos de mensagens para comunicação sobre andamento de casos

As funcionárias de LAWRS podem se comunicar com as usuárias por telefone ou aplicativos de mensagens (como o WhatsApp) usando telefones celulares fornecidos por LAWRS. Essa comunicação é regida pelo Regulamento Geral de Proteção de Dados do Reino Unido (UK GDPR), pela Lei de Proteção de Dados de 2018 e pelas obrigações de confidencialidade de LAWRS.

1. Consentimento e momento da comunicação

- Antes de iniciar o contato por telefone ou WhatsApp, as funcionárias devem obter o consentimento expresso da usuária de serviços, incluindo seu método preferido, data e hora para comunicação.
- Essa preferência deve ser documentada no Lamplight e revisada regularmente.

2. Uso de intérpretes

- Quando for necessária uma intérprete para a comunicação, ela deve ser totalmente informada e concordar em cumprir os princípios do UK GDPR, incluindo confidencialidade, limitação de propósito e minimização de dados.
- Os intérpretes não podem reter ou registrar quaisquer dados pessoais compartilhados durante chamadas ou sessões e devem confirmar por escrito sua concordância com os termos de proteção de dados de LAWRS antes de prestar assistência.

3. Dispositivos permitidos

- De preferência, apenas celulares fornecidos por LAWRS devem ser usados para comunicação com as usuárias de serviços. Celulares pessoais nunca devem ser usados para armazenar ou compartilhar dados das usuárias de serviços.

4. Aplicativos e ferramentas permitidos

- Chamadas, SMS e WhatsApp podem ser usados para comunicação limitada e apropriada (por exemplo, agendamento, atualizações breves).
- O WhatsApp é permitido devido à sua criptografia de ponta a ponta.

5. Manutenção de registros

- Qualquer conversa relevante (por exemplo, planejamento de sessões, atualizações sobre crises) deve ser resumida no Lamplight no mesmo dia.
- Os pontos principais das mensagens do WhatsApp devem ser registrados (por exemplo, "Compromisso confirmado pelo WhatsApp em 04/06 às 14:00"). Capturas de tela não substituem o registro.

6. Segurança e confidencialidade

- Os telefones LAWRS devem ser protegidos por uma senha forte ou bloqueio biométrico e bloqueio automático após inatividade.

- Os telefones não devem ser deixados sem supervisão em espaços compartilhados.
- Qualquer perda ou roubo deve ser comunicado imediatamente às DPOs para que o dispositivo possa ser apagado remotamente.

7. Segurança da usuária de serviços

- As funcionárias devem verificar se é seguro ligar ou enviar mensagens à usuária. Se a pessoa compartilha seu telefone ou vive em um ambiente controlado, alternativas mais seguras (por exemplo, e-mail codificado ou acompanhamento pessoal) devem ser utilizadas.

8. Retenção e exclusão

- As funcionárias devem excluir regularmente as mensagens do WhatsApp dos telefones assim que as informações forem registradas no Lamplight. Mensagens ou capturas de tela não devem ser armazenadas em telefones, backups ou unidades de armazenamento externas.

9. Treinamento e supervisão

- Todas as funcionárias e voluntárias que utilizam telefones LAWRS devem ser treinadas no manuseio de dados móveis e concordar em cumprir esta política.
- As DPOs podem conduzir verificações periódicas e fornecer orientações sobre o uso compatível das ferramentas de comunicação móvel.

4.3 Funcionárias e voluntárias

Os registros de RH das funcionárias e voluntárias (por exemplo, contratos, referências, avaliações de desempenho, verificações DBS) são armazenados separadamente em pastas seguras e com acesso controlado no Google Drive organizacional de LAWRS. Esses registros só podem ser acessados pela equipe de gestão sênior, administradores e gerentes relevantes. O acesso da diretoria aos arquivos das funcionárias é restrito e deve ser justificado e documentado. A coordenadora de voluntárias gerencia os registros das voluntárias, com acesso restrito conforme descrito acima.

4.4 Membras

As informações pessoais das membras serão mantidas no sistema de gerenciamento de casos de LAWRS - Lamplight. As administradoras são responsáveis pelo gerenciamento de seus dados. Embora todas as funcionárias e algumas voluntárias possam ter acesso às informações, apenas as administradoras, a equipe de políticas e comunicações e a equipe de gestão sênior devem processar os dados.

4.5 Conselho Gestor

As informações pessoais das membras do Conselho Gestor serão mantidas no Google Drive. as administradoras são responsáveis pelo gerenciamento das informações, enquanto as administradoras e a equipe de gestão sênior têm acesso às suas informações.

Como regra geral e de acordo com o compromisso da nossa organização com a transparência e a responsabilidade, as atas, relatórios e propostas do Conselho Gestor são documentos compartilhados e abertos, exceto quando um item confidencial está sendo discutido.

Quando documentos marcados como “Privados e Confidenciais” são discutidos nas reuniões do Conselho Gestor, eles não podem ser compartilhados com terceiros sem o consentimento expresso da pessoa relevante. As atas de itens confidenciais serão mantidas separadamente das atas principais da reunião.

As membras do Conselho Gestor não devem discutir assuntos confidenciais abordados nas reuniões fora delas.

4.6 Sistema de gerenciamento de casos Lamplight – Aviso do processador de dados

LAWRS é a controladora de dados para todos os dados pessoais inseridos no sistema de gerenciamento de casos Lamplight. A Lamplight Database Systems Ltd atua como processadora de dados, e a Amazon Web Services (AWS) atua como subprocessadora, fornecendo a infraestrutura de hospedagem em nuvem.

Localização da hospedagem – Os dados primários e de backup residem nas regiões AWS EU-West (República da Irlanda e, para resiliência, outros centros de dados da UE). Não são feitas transferências de rotina para fora do Reino Unido/EEA.

Salvaguardas contratuais – O processamento é regido pelo Acordo de Processamento de Dados (DPA, v 2024-12) da Lamplight, que incorpora:

Adendo de Transferência Internacional de Dados do Reino Unido (IDTA) e Cláusulas Contratuais Padrão da UE para quaisquer transferências subsequente;

Termos de Serviço da AWS e Adendo de Proteção de Dados (última atualização em 1 de fevereiro de 2025).

Medidas de segurança – A AWS é certificada pela ISO 27001, SOC 2 Tipo II e emprega criptografia em repouso (AES-256) e em trânsito (TLS 1.2+). A Lamplight aplica controle de acesso baseado em funções, MFA, backups criptografados diários e testes de restauração trimestrais.

Auditoria e exclusão – LAWRS reserva-se o direito de solicitar relatórios de auditoria resumidos ou de contratar uma inspeção por terceiros. Após o término do contrato, a Lamplight, a critério de LAWRS, devolverá ou apagará com segurança todos os dados pessoais dentro de 30 dias.

4.7 Gravações de reuniões com inteligência artificial e ferramentas de transcrição

Devido à natureza sensível do trabalho realizado por LAWRS, incluindo o processamento regular de dados pessoais confidenciais e de categorias especiais, não é permitido o uso de ferramentas de transcrição com inteligência artificial (IA) ou qualquer forma de gravação de reuniões (áudio ou vídeo) com inteligência artificial (IA). Isso se aplica a todas as reuniões internas e externas envolvendo usuárias, funcionárias, voluntárias ou terceiros.

LAWRS adotou esta posição para proteger a privacidade, dignidade e segurança das pessoas e para garantir o pleno cumprimento do RGPD do Reino Unido, em particular os artigos 5.º e 9.º, relativos à minimização, integridade, confidencialidade e processamento de dados de categorias especiais.

5. Mídia

Qualquer membro da mídia que entrar em contato com LAWRS deve ser encaminhado inicialmente à Diretora. A diretora pode fornecer informações sobre o trabalho e posicionamento de LAWRS e autorizar uma funcionária a fazer o mesmo. Fica a critério da diretora decidir se compartilhará ou não tais informações e avaliar os benefícios e possíveis riscos.

Quando a diretora não estiver presente, o vice-diretora ou uma funcionária designada pela diretora avaliará se é apropriado compartilhar informações com a imprensa, emissoras de rádio e TV ou mídia eletrônica, bem como os possíveis benefícios e riscos. No entanto, informações pessoais não devem ser compartilhadas, a menos que LAWRS tenha o consentimento expresso da pessoa envolvida.

LAWRS pode compartilhar informações anonimizadas com a mídia ou imprensa, qualquer outra organização ou com o público em geral, se a diretora considerar legal e apropriado, sem o consentimento expresso da pessoa. A anonimização envolve a remoção de todas as informações identificadoras para que a pessoa não possa mais ser reconhecida. Antes de qualquer tipo de divulgação, LAWRS deve avaliar cada situação em particular, equilibrando os riscos e os benefícios. A diretora ou a pessoa designada pela diretora deve decidir qual processo usar em cada circunstância, como, mas não se limitando ao uso de um pseudônimo, mudança da nacionalidade, idade, número de membros da família e assim por diante. A organização também deve considerar como LAWRS e suas usuárias se beneficiariam com o compartilhamento de tais informações.

6. Pesquisa

As usuárias, voluntárias e funcionárias devem receber as seguintes informações antes de participarem de pesquisas realizadas por ou por meio de LAWRS:

- Responsável pela pesquisa e detalhes de contato
- Informações sobre instituições parceiras
- Tópico da pesquisa
- Política de anonimato da pesquisa
- Direito de retirar o consentimento a qualquer momento
- Planos de divulgação
- Direito das participantes de retirar o consentimento em qualquer fase da pesquisa

No momento da obtenção do consentimento, todas as usuárias de serviços serão informadas de que “LAWRS utilizará dados anonimizados, através dos quais a usuária não é identificável, para melhorar os serviços, para reportar aos financiadores, para fins de pesquisa e para aumentar a conscientização de doadores, parceiros, público em geral e outros sobre os problemas que afetam as usuárias de seus serviços”.

7. Dados estatísticos

LAWRS pode manter registros estatísticos das pessoas para monitorar os serviços prestados e as necessidades da comunidade. As informações estatísticas serão fornecidas de forma anônima, portanto, a pessoa não será identificada.

Os gerentes de cada projeto são responsáveis por avaliar quaisquer informações pessoais fornecidas para análise estatística a terceiros, tais como, mas não exclusivamente: em apoio a pedidos de subsídios, para fins de relatórios, etc.

8. E-mails, telefone e correio

LAWRS deve perguntar às pessoas se elas querem ser contatadas por LAWRS. As funcionárias devem perguntar qual é o método de contato preferido da usuária e o tipo de informação que querem receber. Se uma usuária da VAWG for contatada por telefone, as funcionárias e as voluntárias devem garantir que LAWRS não seja mencionada ao deixar mensagens ou se comunicar com outras pessoas que não sejam da usuária.

A funcionária ou voluntária que distribuir a correspondência deve manter as informações confidenciais, de acordo com a legislação de proteção de dados e as políticas de LAWRS. A correspondência endereçada à LAWRS será aberta por uma funcionária ou voluntária sob a supervisão de uma funcionária, que decidirá a quem será entregue.

Para evitar a violação desta política, o seguinte parágrafo deve ser incluído em cada e-mail enviado pela organização:

“As informações incluídas neste e-mail são confidenciais e destinam-se ao uso exclusivo do destinatário nomeado. Se você recebeu este e-mail por engano, entre em contato conosco imediatamente.

9. Exceções

LAWRS pode compartilhar informações pessoais de indivíduos em determinadas circunstâncias. Assim, se alguma funcionária ou voluntária identificar qualquer tipo de dano pessoal, risco de dano pessoal, abuso, negligência ou sinais de violência física ou psicossocial, incluindo abuso emocional a si mesmo ou a outros, LAWRS deverá relatar a questão à polícia, assistentes sociais ou à instituição apropriada. Além disso, quando houver conhecimento de que uma criança está sendo abusada ou corre o risco de ser abusada, ou quando houver informações sobre um adulto vulnerável em risco,

funcionárias ou voluntárias seguirão o procedimento estabelecido na política e procedimento de proteção e salvaguarda de LAWRS ou na política e procedimento de proteção de adultos.

Pode haver outras circunstâncias em que LAWRS seja obrigada por lei a compartilhar informações pessoais, por exemplo, para cumprir uma ordem judicial após ser notificada.

10. Sanções em caso de quebra da confidencialidade

LAWRS reconhece que muitas das quebras de confidencialidade não são intencionais e podem ocorrer quando uma conversa é ouvida por terceiros, um arquivo é deixado sem vigilância ou quando os sistemas de TIC não dispõem das medidas de segurança adequadas. No entanto, tais incidentes serão considerados tão graves quanto aqueles cometidos deliberadamente.

Quando uma funcionária compartilha informações confidenciais com terceiros, viola esta política ou há suspeita de violação, ela deve:

- Preencher e enviar o formulário para informar quebra de confidencialidade (Apêndice 3) à sua gerente imediata e à DPO por e-mail assim que a quebra de confidencialidade for identificada.

Assim que o formulário de quebra de confidencialidade for recebido, a DPO investigará o incidente, avaliará os riscos que ele pode representar e elaborará um plano com as próximas etapas dentro de 72 horas a partir do momento em que a quebra de confidencialidade foi identificada.

A DPO então processará e executará qualquer ação relevante, dependendo da gravidade e do risco que representa para o(s) indivíduo(s) afetado(s). O Gabinete do Comissário de Informação (ICO) e as pessoas envolvidas devem ser contactados através do formulário e e-mail apropriados dentro do mesmo prazo, e um registro do pedido deve ser feito no sistema de gestão de casos de LAWRS.

O resultado desta investigação pode exigir um procedimento disciplinar, de acordo com as regras estabelecidas na política e procedimento de reclamação, disciplinar e denúncia.

LAWRS procurará resolver os pedidos no prazo de 72 horas. Se isso não for possível, por qualquer motivo, deverá ser enviada uma atualização do andamento do processo tanto à ICO como às pessoas afetadas, indicando quando se poderá esperar uma resposta completa.

Em caso de quebra de confidencialidade pelo Diretora, será da responsabilidade da Presidenta, ou, se este não estiver disponível, de uma membra do Conselho Gestor, seguir o procedimento de quebra de confidencialidade, preencher o formulário de quebra de confidencialidade e realizar a investigação e, potencialmente, um

procedimento disciplinar, de acordo com as regras estabelecidas na política e procedimento de reclamação, disciplinar e denúncia.

Quando uma voluntária compartilha informações confidenciais com terceiros ou viola esta política, isso deve ser relatado imediatamente à coordenadora de voluntárias e à DPO, seguindo o procedimento de quebra de confidencialidade e preenchendo o formulário de quebra de confidencialidade. Dependendo da gravidade da quebra de confidencialidade, pode ser decidido que essa pessoa não deve mais ser voluntária e deve deixar a organização por completo.

No caso das membras do Conselho Gestor, caberia ao Conselho Gestor decidir quais medidas tomar em relação 'a membra que violou a confidencialidade, levando em consideração a gravidade da quebra de confidencialidade e os danos potenciais à reputação de LAWRS. O procedimento de quebra de confidencialidade deve ser aplicado.

LAWRS tem o dever de comunicar as violações de dados à ICO no prazo de 72 horas, se a quebra de confidencialidade for suscetível de resultar num risco para os direitos e liberdades das pessoas, tais como discriminação, danos à reputação ou perdas financeiras. Eventualmente, se a quebra de confidencialidade for suscetível de resultar num risco elevado para os direitos e liberdades da pessoa, deve também ser notificada diretamente à pessoa em causa, sem demora injustificada. A diretora ou a pessoa designada será responsável por gerenciar o processo.

11. Procedimento de reclamações

O procedimento de reclamação de LAWRS, conforme estabelecido na política e procedimento de reclamações de LAWRS, oferece um mecanismo através do qual qualquer indivíduo pode expressar seu desacordo ou preocupação em relação a qualquer questão relacionada à gestão de dados.

Se um indivíduo não estiver satisfeito com a nossa resposta à reclamação, ela pode entrar em contato com a ICO, que supervisiona a proteção de dados pessoais no Reino Unido, ou com o Regulador de Captação de Recursos, responsável pela supervisão das atividades de arrecadação de fundos realizadas por instituições de caridade no Reino Unido.

12. Lei de Proteção de Dados

LAWRS cumpre todas as obrigações legais estabelecidas no RGPD do Reino Unido, na Lei de Proteção de Dados de 2018 e nos Regulamentos de Privacidade e Comunicações Eletrônicas (PECR). Portanto, a coleta, o processamento e o armazenamento de informações pessoais são feitos de acordo com essa legislação. LAWRS garantirá o cumprimento da lei por meio das seguintes medidas:

- Informando todas as pessoas sobre as responsabilidades decorrentes da lei como parte do processo de integração.

- Mantendo as pessoas atualizadas sobre qualquer alteração nas suas obrigações legais nos termos da lei.

13. Registro de Atividades de Processamento (ROPA) e Destruição de Dados

A destruição das informações pessoais coletadas e armazenadas por LAWRS será feita da seguinte maneira, a menos que exigido por obrigações legais:

	ATIVIDADE DE PROCESSAMENTO	Artigo 6º Base legal	Condição de categoria especial do art. 9	Dados típicos mantidos	Período de gatilho de retenção
1	Aconselhamento , defesa e documentação de caso	6(1)(b) Contrato (serviço solicitado pela usuária)	9(2)(d) Sem fins lucrativos com salvaguardas	Detalhes de contato, status imigratório , saúde, detalhes de filhos , encaminhamentos, notas de caso	6 anos após o último registro de caso (os detalhes do contrato da creche armazenados no Google Drive serão excluídos 1 ano após o último acesso ao serviço da creche)
2	Encaminhamento ou divulgações de proteção (não registradas no Lamplight, conforme especificado nas políticas de proteção de LAWRS)	6(1)(d) Interesses vitais	9(2)(c) Interesses vitais	Como acima + notas de risco	Até a conclusão da investigação legal + 1 ano
3	Recrutamento	6(1)(f) Interesses legítimos	Base do artigo 10 da DPA 2018, Anexo 1, Parte 1, parágrafo 1 – Emprego e proteção	CV, detalhes de contato, notas de entrevista, formulários de candidatura	6 meses após o término do recrutamento
4	Monitoramento de igualdade de oportunidades e	6(1)(f) Interesses legítimos	9(2)(g) Interesse público	Etnia, orientação sexual,	Anonimizar após o relatório anual e, em seguida,

	impacto (funcionárias e voluntárias candidatas a emprego)		substancial – igualdade	deficiência	excluir os dados brutos
5	Atualizações por e-mail, SMS e correio sobre os serviços de LAWRS	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, e-mail, preferência de idioma	Até que o consentimento seja retirado ou 2 anos de inatividade
6	Gestão de RH e Voluntariado	6(1)(b) Contrato	9(2)(b) Direito laboral e da segurança social	Referências, verificações DBS, informações de saúde, formulários de candidatura para voluntárias (formulário do Google)	6 anos para funcionárias e 2 anos para voluntárias - após o término do emprego/voluntariado
7	Registros do Conselho Gestor e de governança	6(1)(c) Obrigação legal (Lei das Sociedades, Lei das Instituições de Caridade)	n / D	Detalhes de contato das membras do conselho gestor, atas	Ata da diretoria – permanente; dados pessoais – 6 anos após o mandato
8	Registros de incidentes de saúde e segurança	6(1)(c) Obrigação legal	9(2)(f) Demandas legais	Relatórios de lesões, declarações de testemunhas	40 anos a partir do incidente (regulamentos de responsabilidade da empregadora)
9	Respostas do formulário do Google para eventos	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, endereço de e-mail, número de telefone, data de nascimento, idioma	Incluir dados anonimizados no Lamplight e excluir dados após o evento

10	Formulário do Google (encaminhamentos)	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, endereço de e-mail, número de telefone, data de nascimento, idioma	Carregar resposta no Lamplight e eliminar resposta
11	Registros de Reclamações	6(1)(f) Interesses legítimos	N/A (a menos que a reclamação inclua dados de categoria especial – então 9(2)(f) Demandas legais)	Nome do reclamante, detalhes de contato, detalhes do incidente, notas do caso, resultados	3 anos após a resolução da reclamação
12	Pesquisa e coleta de evidências	6(1)(f) Interesses legítimos	9(2)(j) Fins de pesquisa com salvaguardas (se forem utilizados dados pessoais)	Respostas de pesquisas, dados anônimos de usuáries de serviços, informações demográficas	5 anos após a publicação
13	Informações sobre fornecedores, prestadores e contratados	6(1)(b) Contrato	n / D	Nome, detalhes de contato comercial, termos do contrato, registros de pagamento	6 anos após o término do contrato (conforme Lei de Prescrição de 1980)
14	Informações contábeis e financeiras	6(1)(c) Obrigação legal (Lei das Finanças de 1998, Lei das Sociedades de 2006)	n / D	Faturas, folha de pagamento, recibos, relatórios orçamentários	6 anos a partir do final do ano fiscal (conforme orientação do HMRC)

15	Contratos de apólices de seguro	6(1)(c) Obrigação legal	n / D	Documentos de apólice, termos de cobertura	6 anos a partir do vencimento da apólice
16	Apólices de seguro de responsabilidade civil da empregadora	6(1)(c) Obrigação legal	n / D	Nome da seguradora, detalhes da cobertura, números de certificados	40 anos a partir do vencimento da apólice
17	Documentação de apoio para projetos financiados pela UE	6(1)(c) Obrigação legal (condições de subvenção UE/Reino Unido)	n / D	Planos de projeto, registros de trabalhadoras, orçamentos, registros de participantes	cinco anos após o último pagamento/recuperação da UE para o projeto.

A destruição de informações em papel será feita com uma trituradora de papel ou contratando uma empresa de trituração certificada, sob a supervisão da Diretora. A destruição de informações mantidas digitalmente será feita excluindo-as da nuvem (sistema de gerenciamento de casos e unidade organizacional).

14. Avaliação do Impacto na Proteção de Dados (DPIA)

Em conformidade com o Regulamento Geral de Proteção de Dados do Reino Unido (UK GDPR), LAWRS realizará uma Avaliação do Impacto na Proteção de Dados (DPIA) antes de introduzir qualquer novo serviço, projeto ou mudança nas práticas de trabalho que envolva o processamento de dados pessoais, particularmente dados sensíveis ou de categoria especial. O propósito da DPIA é identificar potenciais riscos à proteção de dados, garantir que salvaguardas adequadas estejam em vigor, demonstrar conformidade com a lei de proteção de dados e proteger os direitos das usuárias de serviços, funcionárias, voluntárias e membras do público. A DPIA será liderada pelos DPOs em parceria com o líder da atividade ou serviço relevante, iniciada no máximo duas semanas antes do início planejado da nova atividade ou serviço, revisada e arquivada antes do início de qualquer processamento.

Todas as DPIA serão documentadas e mantidas em arquivo como parte das obrigações de responsabilidade de LAWRS nos termos do artigo 35.º do RGPD do Reino Unido.

Aprovado pelo Conselho gestor de LAWRS:

Assinatura da presidenta

Assinatura da secretária

Apêndice 1: Formulário de consentimento da usuária de serviços

Formulário de consentimento da usuária de serviços

De acordo com a legislação vigente (Lei de Proteção de Dados de 2018 e RGPD do Reino Unido), LAWRS requer seu consentimento explícito para processar, registrar e armazenar seus dados pessoais, incluindo dados de categorias especiais, como informações relacionadas à sua saúde, etnia, status migratório, informações familiares ou outros assuntos confidenciais relevantes para o apoio que prestamos.

Suas informações pessoais serão armazenadas com segurança em papel ou eletronicamente e tratadas como confidenciais, acessíveis apenas por funcionárias e voluntárias relevantes, com as seguintes exceções:

- Quando você nos **solicitar expressamente para entrar em contato** com outros serviços ou organizações em seu nome. O propósito e a natureza de qualquer informação que possa ser compartilhada serão discutidas com você antes de qualquer contato.
- Quando a funcionária identificar **risco** de dano a você ou a outras pessoas, especialmente crianças ou adultos vulneráveis, incluindo exposição potencial a qualquer forma de negligência ou abuso, em conformidade com a legislação do Reino Unido.
- De acordo com os requisitos profissionais e éticos, as funcionárias podem discutir seu trabalho com **supervisores** externos para garantir a qualidade do serviço.
- Quando exigido por **auditorias e verificações de qualidade**.

Um código único será atribuído a você para preservar sua identidade.

LAWRS também utiliza dados anonimizados, através dos quais as pessoas não são identificáveis, para melhorar os serviços, para relatar aos financiadores, para fins de pesquisa e para aumentar a conscientização dos doadores, parceiros, público em geral e outros sobre os problemas que afetam as usuárias de seus serviços.

Você tem o direito de retirar seu consentimento e solicitar acesso aos seus arquivos com aviso prévio, o que, em alguns casos, pode afetar a capacidade de LAWRS de fornecer alguns serviços. As informações pessoais das usuárias de serviços serão destruídas após seis anos, a menos que exigido por lei ou por um motivo excepcional, conforme estabelecido na Política de Confidencialidade e Proteção de Dados de LAWRS.

Gravações de voz, vídeo ou qualquer outro tipo de gravação sem o consentimento explícito e acordado por todas as partes são estritamente proibidas e podem resultar no cancelamento imediato da prestação de serviços.

Para mais informações, solicite uma cópia da Política de Confidencialidade e Proteção de Dados de LAWRS a qualquer funcionária, por e-mail, em lawrs@lawrs.org.uk.

Dou meu consentimento ao Serviço pelos Direitos da Mulher Latino-americana "LAWRS" para:

	Registrar, processar e armazenar informações pessoais e confidenciais sobre mim para os fins mencionados neste formulário.
	Entendo que informações editadas, que não me identifiquem, podem ser incluídas nas comunicações públicas de LAWRS e nos relatórios dos financiadores.

	Sei que tenho o direito de ver as informações se solicitar e de retirar o meu consentimento.
	Compreendo que devo fornecer informações verdadeiras, de acordo com o meu melhor conhecimento, e que, caso contrário, posso deixar de ser apoiado por LAWRS.
	Concordo em ser contactada por LAWRS pessoalmente, por telefone, por e-mail ou por mensagem de texto para receber informações sobre as atividades, campanhas, notícias, vagas de emprego, etc. de LAWRS.
	Dou minha permissão expressa para que fotos ou filmagens minhas, gravadas durante a participação em atividades organizadas por LAWRS, sejam utilizadas em publicações, campanhas, materiais, anúncios, materiais de exibição, materiais eletrônicos, trabalhos de mídia, etc.

Apêndice 2: Formulário de solicitação de dados pessoais

Formulário de solicitação de dados

pessoais

(para uso interno)

Pessoa que recebe a solicitação:	
Função na organização:	
Data e hora da solicitação:	
Tipo:	
☐	Solicitação de retirada de consentimento
☐	Solicitação de direito de exclusão
☐	Solicitação de acesso do titular dos dados

Dados da requerente:

Nome:	
Telefone:	
Endereço:	
E-mail:	
Meio de comunicação preferencial:	Correio E-mail
☐ Identidade verificada (necessário apenas se o pedido for feito por alguém que não seja conhecido anteriormente por LAWRS)	

Use o espaço abaixo para descrever as circunstâncias da solicitação e quaisquer outras informações relevantes.

Explique com o máximo de detalhes possível o motivo da solicitação (por exemplo: especifique qual consentimento o solicitante deseja retirar; quais dados pessoais o solicitante deseja que sejam excluídos; a quais informações o solicitante deseja ter acesso).

Breve explicação do procedimento e prazos após a solicitação ser feita:

Solicitação de retirada de consentimento: formulário só precisa ser preenchido se a retirada do consentimento estiver relacionada aos tópicos 1, 2, 3 e 4, pois isso pode afetar a capacidade de LAWRS de fornecer alguns serviços. Para os tópicos 5 e 6 do formulário de consentimento, as solicitações de retirada podem ser processadas imediatamente e registradas diretamente no sistema de gerenciamento de casos de LAWRS.

Tópicos do formulário de consentimento	
1.	Registrar, processar e armazenar informações pessoais e confidenciais sobre mim para os fins mencionados neste formulário.
2.	Entendo que informações editadas, que não me identificariam, podem ser incluídas nas comunicações públicas de LAWRS e nos relatórios dos financiadores.
3.	Ser que tenho o direito de ver as informações se solicitar e de retirar meu consentimento.
4.	Compreendo que preciso fornecer informações verdadeiras, de acordo com o meu melhor conhecimento, e que, caso contrário, posso não continuar a receber o apoio de LAWRS.
5.	Concordo em ser contactado por LAWRS pessoalmente, por telefone, por e-mail ou mensagem de texto para receber informações sobre as atividades, campanhas, notícias, vagas de emprego, etc. de LAWRS.
6.	Dou minha permissão expressa para que fotos ou filmagens minhas, gravadas durante a participação em atividades organizadas por LAWRS, sejam utilizadas em publicações, campanhas, materiais, anúncios, materiais de exibição, materiais eletrônicos, trabalhos de mídia, etc.

Ação	Prazo
A gerente e a DPO devem ser informados	no mesmo dia da solicitação
Ambos devem avaliar os possíveis efeitos que isso pode ter na prestação de serviços do solicitante	7 dias úteis a partir da data da solicitação
A DPO deve informar o solicitante sobre as conclusões. Confirmar se ela deseja prosseguir	8 dias úteis a partir da data da solicitação
A DPO deve atualizar o sistema de gerenciamento de casos de LAWRS	assim que a solicitante for contatado

Direito de Solicitação de Esquecimento : LAWRS reserva-se o direito de negar ou aceitar parcialmente a solicitação. Alguns dados podem ter que ser mantidos para cumprir uma obrigação legal.

Ação	Prazo final
A gerente e a DPO devem ser informados	mesmo dia da solicitação

A DPO deve solicitar à gerente Sênior que confirme se há algum dado pessoal que não possa ser excluído (a gerente sênior se baseará no contrato/acordo assinado com o financiador)	dentro de 2 dias úteis a partir do dia da solicitação
A gerente sênior deve informar a DPO sobre as descobertas.	15 dias úteis a partir da data da solicitação
A DPO deve informar ao solicitante quais dados serão apagados e mantidos e por quê	20 dias úteis a partir da data da solicitação
A DPO atualizará o sistema de gerenciamento de casos de LAWRS	20 dias úteis a partir da data da solicitação

Solicitação de Acesso à Titular: LAWRS deve responder à solicitação no prazo de **um mês**. Se a solicitação for complexa, LAWRS poderá precisar de mais tempo para analisá-la e pode levar até **dois meses a mais** para responder.

Todas as informações pessoais da usuária de serviços serão destruídas após 6 anos do encerramento do caso.

Ação	Prazo final
A gerente e a DPO devem ser informados	mesmo dia da solicitação
A DPO deve informar a gerente Sênior sobre a solicitação	dentro de 2 dias úteis a partir do dia da solicitação
A gerente sênior deve coletar os dados solicitados, avaliar os riscos potenciais que elas podem apresentar à usuária (por exemplo: produzir evidências contra si mesmo) e informar a DPO	15 dias úteis a partir da data da solicitação
A DPO deve informar o solicitante sobre os riscos potenciais e confirmar se deseja prosseguir com a solicitação	20 dias úteis a partir da data da solicitação
A DPO enviará informações solicitadas ao solicitante e atualizará o sistema de gerenciamento de casos de LAWRS	30 dias úteis a partir da data da solicitação
Se não houver resolução no prazo de 30 dias, a DPO deverá informar a requerente sobre a extensão e a justificativa para tal.	Se a solicitação não puder ser concluída dentro de um mês civil, a DPO notificará a pessoa até o dia 30 com uma explicação e um prazo revisado, não excedendo dois meses adicionais.

Declaração do Requerente

Declaro que:

- Fui informada sobre a política de confidencialidade e proteção de dados de LAWRS e uma cópia foi disponibilizada para mim.
- Recebi uma breve explicação sobre a política de confidencialidade e proteção de dados de LAWRS, incluindo o que acontecerá em seguida e o tempo estimado para resolução.
- Entendo que, embora o objetivo de LAWRS seja resolver as solicitações o mais rápido possível, em alguns casos, pode haver circunstâncias extraordinárias que podem atrasar a resolução. Nesses casos, LAWRS manterá a solicitante atualizada durante todo o processo.
- Ao melhor do meu conhecimento, tudo o que disse é correto.

- O conteúdo registrado neste formulário foi lido para mim e concordo com ele.
- Entendo que, para ajudar a resolver minha solicitação, LAWRS precisará usar e manter informações pessoais sobre mim – por exemplo, como entrar em contato comigo e detalhes sobre minha solicitação e, às vezes, informações pessoais confidenciais.
- Entendo que, exceto em circunstâncias excepcionais, faremos todos os esforços para garantir que tanto eu quanto LAWRS mantenhamos a confidencialidade. No entanto, as circunstâncias que deram origem à solicitação podem impossibilitar a manutenção da confidencialidade (com cada solicitação sendo avaliada com base em seus próprios méritos). Nesse caso, a situação me será explicada.

Assinatura:

Nome impresso:

Data:

Última atualização do formulário: julho de 2025

Apêndice 3: Formulário para informar quebra de confidencialidade

Formulário para informar quebra de confidencialidade
(para uso interno)

Preencha este formulário se algum dado pessoal tiver sido vazado ou houver suspeita de quebra de confidencialidade.

Pessoa relatando:
Função na organização:
Data e hora em que ocorreu:
Data e hora em que foi identificado:
Tipo de vazamento de dados:

Detalhes da pessoa afetado (adicione mais indivíduos, se necessário):

Indivíduo nº 1

Nome:
ID do Lamplight:

Indivíduo nº 2

Nome:
ID do Lamplight:

Use o espaço abaixo para anotar as circunstâncias da quebra de confidencialidade ou potencial quebra de confidencialidade, quais dados foram violados e qualquer outra informação relevante

Por favor, explique com o máximo de detalhes possível como você descobriu a quebra de confidencialidade, o que aconteceu, como aconteceu e quais informações vazaram.

--

Breve explicação sobre o que acontecerá após a quebra de confidencialidade ser identificada e os prazos:

Linha do tempo	Prazo final
1. Formulário completo	quando a quebra de confidencialidade foi identificada
2. A gerente e a DPO devem ser informados	mesmo dia
3. Investigação a ser conduzida pela DPO para avaliar riscos e próximos passos	dentro de 72 horas
4. Dependendo da gravidade e do risco que isso representa para o(s) indivíduo(s) afetado(s), o ICO e o(s) indivíduo(s) serão contatados.	72 horas
5. DPO deve atualizar a Lamplight caso a pessoa tenha sido notificada	assim que a notificação for feita
6. Possível implementação de mudanças para evitar futuras violações	O mais breve possível
7. O procedimento disciplinar, de acordo com a política e procedimento de reclamação, disciplina e denúncia, poderá ser seguido	após a conclusão da investigação



Apêndice 4: Orientações sobre o envio de e-mails em massa pelo Lamplight

Orientações sobre o envio de e-mails em massa pelo Lamplight

Para evitar vazamento de dados e garantir a conformidade com as permissões de contato das usuárias, e-mails em massa devem ser enviados somente pelo Lamplight.

* **Observação:** isso não se aplica à equipe de comunicação, que pode continuar usando sua própria lista de mala direta por meio de uma plataforma de mala direta diferente.

Antes de enviar e-mails em massa, certifique-se de que sua conta de e-mail esteja devidamente vinculada ao Lamplight, conforme as instruções da equipe de administração.

Depois que sua conta de e-mail estiver configurada, siga estas etapas para enviar e-mails em massa pelo Lamplight:

1. Entre na sua conta Lamplight.
2. Clique na aba “Salvar” na parte superior da tela.
3. Selecione “Comunicação” e clique em “Criar”.
4. Selecione “Email” (a primeira opção da lista).
5. No campo “Resumo para salvar”, inclua uma breve descrição do tópico do e-mail e clique em “Avançar”.
6. Na aba “2. Destinatários”, insira os números de perfil ou nomes completos das usuárias que você deseja contatar. Selecione quantos forem necessários. À medida que você os seleciona, seus nomes e endereços de e-mail aparecerão em uma caixa abaixo.

Observação: as usuárias que optaram por não receber e-mails ou

comunicações em massa não terão seus endereços de e-mail listados, o que significa que o sistema não enviará o e-mail a elas, mesmo se selecionado.

7. Depois de escolher todos os destinatários, clique em “Avançar”.
8. Na aba “Detalhes do e-mail”:
 - Digite o assunto do e-mail sem usar acentos (acentos no assunto podem não ser exibidos corretamente para as destinatárias). Os acentos ainda podem ser usados no corpo do e-mail.
 - O campo "Endereço de e-mail do remetente" será preenchido automaticamente com o e-mail que você registrou no Lamplight.
 - O campo "Nome de exibição do remetente" será preenchido automaticamente com o nome da organização, mas devido aos limites de caracteres, recomendamos alterá-lo para "LAWRS" em vez de "Latin American Women's Rights Service".
 - Para e-mails em massa, no campo “Como você deseja enviar os e-mails?”, escolha sempre a segunda opção: “Um único e-mail com cópia oculta (Cco) para todos os destinatários”. Em seguida, clique em “Avançar”.
9. Na aba "Arquivos", anexe os arquivos necessários clicando em "Escolher arquivo". Você pode anexar até 7 arquivos por e-mail. Clique em "Avançar".
10. Na aba "Conteúdo da mensagem", escreva o corpo do seu e-mail. Recomenda-se revisar o conteúdo pelo menos duas vezes para verificar se há erros de digitação ou outros erros. Ao terminar, clique em "Criar/Enviar" no canto inferior direito.

Dica: É altamente recomendável testar o processo enviando um e-mail de teste para você mesmo. Isso ajuda a garantir que o e-mail esteja formatado corretamente e que todos os anexos cheguem conforme o esperado.

Última atualização do formulário: julho de 2025

Apêndice 5: AVISO DE PRIVACIDADE DE LAWRS (PARA USUÁRIAS DE SERVIÇOS E PÚBLICO EM GERAL)

Aviso de privacidade do cliente do Serviço pelos Direitos da Mulher Latino-americana

Este aviso de privacidade informa o que você pode esperar que façamos com suas informações pessoais.

- Detalhes de contato
- Quais informações coletamos, usamos e por quê
- Bases legais e direitos de proteção de dados
- De onde obtemos informações pessoais
- Por quanto tempo mantemos as informações
- Com quem compartilhamos informações
- Como reclamar

Detalhes de contato

Correio: Serviço pelos Direitos da Mulher Latino-americana, 52-54 Featherstone Street, LONDRES, EC1Y 8RT, GB

Telefone: 0808 145 4909

E-mail: lawrs@lawrs.org.uk

Quais informações coletamos, usamos e por quê

Coletamos ou usamos as seguintes informações para fornecer serviços, incluindo entrega e indicações de terceiros:

- Nomes e detalhes de contato
- Gênero
- Preferências de pronomes
- Endereços
- Data de nascimento
- Detalhes de contato de emergência
- Detalhes do parente mais próximo
- Gravações de chamadas
- Histórico de uso do serviço
- Informações de saúde (incluindo condições médicas, resultados de testes, alergias, requisitos médicos e histórico médico)
- Informações sobre necessidades de cuidados (incluindo deficiências, condições de moradia, necessidades alimentares e cuidados gerais)
- Informações sobre trabalho, moradia e condições de vida
- Informações sobre requisitos de apoio Dados de infrações criminais
- Registros de reuniões e decisões
- Informações sobre renda e necessidades financeiras para financiamento ou apoio orçamentário pessoal
- Informações da usuária do site (incluindo jornadas da usuária e rastreamento de cookies)

Também coletamos ou usamos as seguintes informações de categorias especiais para fornecer serviços, incluindo entregas e encaminhamentos a terceiros. Essas informações estão sujeitas a proteção adicional devido à sua natureza sensível:

- Origem racial ou étnica
- Informações de saúde

Coletamos ou usamos as seguintes informações para receber doações ou financiamento e organizar atividades de arrecadação de fundos:

- Nomes e detalhes de contato
- Endereços

Coletamos ou usamos as seguintes informações pessoais para atualizações de serviços ou propósitos de marketing:

- Nomes e detalhes de contato
- Endereços
- Preferências de marketing

Também coletamos ou usamos as seguintes informações de categorias especiais para fins de pesquisa ou arquivamento. Essas informações estão sujeitas a proteção adicional devido à sua natureza sensível:

- Origem racial ou étnica

Coletamos ou usamos as seguintes informações pessoais para lidar com dúvidas, reclamações ou demandas:

- Nomes e detalhes de contato
- Endereço

Bases legais e direitos de proteção de dados

De acordo com a lei de proteção de dados do Reino Unido, precisamos ter uma "base legal" para coletar e usar suas informações pessoais. Há uma lista de possíveis bases legais no GDPR do Reino Unido. Você pode descobrir mais sobre bases legais no site do ICO.

A base legal que utilizamos pode afetar seus direitos de proteção de dados, que são resumidamente descritos abaixo. Você pode se informar mais sobre seus direitos de proteção de dados e as isenções que podem ser aplicadas no site do ICO:

- Seu direito de acesso - Você tem o direito de nos solicitar cópias de suas informações pessoais. Você pode solicitar outras informações, como detalhes sobre onde obtemos informações pessoais e com quem as compartilhamos. Existem algumas exceções, o que significa que você pode não receber todas as informações solicitadas. Você pode ler mais sobre isso aqui.
- Seu direito de retificação - Você tem o direito de nos solicitar a correção ou exclusão de informações pessoais que considere imprecisas ou incompletas. Saiba mais sobre isso aqui.
- Seu direito de esquecimento /apagamento - Você tem o direito de nos solicitar a exclusão de suas informações pessoais. Saiba mais sobre isso aqui.

- Seu direito à restrição do processamento - Você tem o direito de nos solicitar a limitação do uso de suas informações pessoais. Saiba mais sobre isso aqui.
- Seu direito de se opor ao processamento - Você tem o direito de se opor ao processamento dos seus dados pessoais. Saiba mais sobre isso aqui.
- Seu direito à portabilidade de dados - Você tem o direito de solicitar que transfiramos as informações pessoais que você nos forneceu para outra organização ou para você. Você pode ler mais sobre isso aqui.
- Seu direito de revogar o consentimento – Quando usamos o consentimento como base legal, você tem o direito de revogar seu consentimento a qualquer momento. Você pode ler mais sobre esse direito aqui.

Se você fizer uma solicitação, devemos responder sem demora injustificada e, em qualquer caso, dentro de um mês.

Para fazer uma solicitação de direitos de proteção de dados, entre em contato conosco usando os detalhes de contato no topo deste aviso de privacidade.

Nossas bases legais para a coleta e uso de seus dados

Nossas bases legais para coletar ou usar informações pessoais para fornecer serviços e produtos, incluindo entrega e encaminhamento a terceiros, são:

- Consentimento, incluindo consentimento explícito para processar dados de categorias especiais - obtivemos sua permissão após fornecermos todas as informações relevantes. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção. Para esclarecer, você tem o direito de revogar seu consentimento a qualquer momento.
- Interesses vitais – a coleta ou o uso das informações é necessário quando a saúde física ou mental ou o bem-estar de alguém está em risco urgente ou grave. Isso inclui a necessidade urgente de alimentos, água, roupas ou abrigo para o sustento da vida. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção e o direito à portabilidade.
- Tarefa pública – precisamos coletar ou usar suas informações para executar uma tarefa prevista em lei, que a lei pretende que seja executada por uma organização como a nossa. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de apagamento e o direito à portabilidade.

Nossas bases legais para coletar ou usar informações pessoais para receber doações ou financiamento e organizar atividades de arrecadação de fundos são:

- Consentimento - obtivemos sua permissão após fornecermos todas as informações relevantes. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção. Para esclarecer, você tem o direito de revogar seu consentimento a qualquer momento.

Nossas bases legais para coletar ou usar informações pessoais para atualizações de serviços ou fins de marketing são:

- Consentimento - obtivemos sua permissão após fornecermos todas as informações relevantes. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção. Para esclarecer, você tem o direito de revogar seu consentimento a qualquer momento.

Nossas bases legais para coletar ou usar informações pessoais para fins de pesquisa ou arquivamento são:

- Consentimento - obtivemos sua permissão após fornecermos todas as informações relevantes. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção. Para esclarecer, você tem o direito de revogar seu consentimento a qualquer momento.

Nossas bases legais para coletar ou usar informações pessoais para lidar com dúvidas, reclamações ou demandas são:

- Consentimento - obtivemos sua permissão após fornecermos todas as informações relevantes. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção. Para esclarecer, você tem o direito de revogar seu consentimento a qualquer momento.
- Obrigação legal – precisamos coletar ou usar suas informações para cumprir a lei. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de apagamento, o direito de objeção e o direito à portabilidade de dados.

De onde obtemos informações pessoais

- Diretamente de você
- Autoridades reguladoras
- Membras da família ou cuidadores
- Outros prestadores de cuidados de saúde
- Serviços sociais
- Organizações de caridade ou do setor voluntária
- Conselhos e outras organizações do setor público

Por quanto tempo mantemos as informações

	ATIVIDADE DE PROCESSAMENTO	Artigo 6º Base legal	Condição de categoria especial do art. 9	Dados típicos mantidos	Período de gatilho de retenção
1	Aconselhamento , defesa e documentação de caso	6(1)(b) Contrato (serviço solicitado pela usuária)	9(2)(d) Sem fins lucrativos com salvaguardas	Detalhes de contato, status imigratório , saúde, detalhes dos filhos, encaminhamentos, notas de caso	6 anos após o último registro de caso (os detalhes do contrato da creche armazenados no Google Drive serão excluídos 1 ano após o último acesso ao serviço da creche)
2	Referências ou divulgações de	6(1)(d) Interesses vitais	9(2)(c) Interesses	Como acima +	Até a conclusão da investigação

	proteção (não registradas no Lamplight, conforme especificado nas políticas de proteção do LAWRS)		vitais	notas de risco	legal + 1 ano
3	Recrutamento	6(1)(f) Interesses legítimos	Base do artigo 10 da DPA 2018, Anexo 1, Parte 1, parágrafo 1 – Emprego e proteção	CV, detalhes de contato, notas de entrevista, formulários de candidatura	6 meses após o término do recrutamento
4	Monitoramento de igualdade de oportunidades e impacto (funcionárias e voluntárias candidatas a emprego)	6(1)(f) Interesses legítimos	9(2)(g) Interesse público substancial – igualdade	Etnia, orientação sexual, deficiência	Anonimizar após o relatório anual e, em seguida, excluir os dados brutos
5	Atualizações por e-mail, SMS e correio sobre os serviços de LAWRS	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, e-mail, preferência de idioma	Até que o consentimento seja retirado ou 2 anos de inatividade
6	Gestão de RH e Voluntariado	6(1)(b) Contrato	9(2)(b) Direito do emprego e da segurança social	Referências, verificações DBS, informações de saúde, formulários de candidatura para voluntárias (formulário do Google)	6 anos para funcionárias e 2 anos para voluntárias - após o término do emprego/voluntariado

7	Registros do conselho e de governança	6(1)(c) Obrigação legal (Lei das Sociedades, Lei das Instituições de Caridade)	n / D	Detalhes de contato das membras do conselho gestor, , atas	Ata da diretoria – permanente; dados pessoais – 6 anos após o mandato
8	Registros de incidentes de saúde e segurança	6(1)(c) Obrigação legal	9(2)(f) Demandas legais	Relatórios de lesões, declarações de testemunhas	40 anos a partir do incidente (regulamentos de responsabilidade da empregadora)
9	Respostas do formulário do Google para eventos	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, endereço de e-mail, número de telefone, data de nascimento, idioma	Incluir dados anonimizados no Lamplight e excluir dados após o evento
10	Formulário do Google (encaminhamentos)	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, endereço de e-mail, número de telefone, data de nascimento, idioma,	Carregar resposta no Lamplight e eliminar resposta
11	Registros de Reclamações	6(1)(f) Interesses legítimos	N/A (a menos que a reclamação inclua dados de categoria especial – então 9(2)(f) Demandas legais)	Nome do reclamante, detalhes de contato, detalhes do incidente, notas do caso, resultados	3 anos após a resolução da reclamação
12	Pesquisa e coleta de evidências	6(1)(f) Interesses legítimos	9(2)(j) Fins de pesquisa com salvaguardas (se forem utilizados dados pessoais)	Respostas de pesquisas, dados anônimos de usuárias de serviços, informações demográfica	5 anos após a publicação

				s	
13	Informações sobre fornecedores, prestadores e contratados	6(1)(b) Contrato	n / D	Nome, detalhes de contato comercial, termos do contrato, registros de pagamento	6 anos após o término do contrato (conforme Lei de Prescrição de 1980)
14	Informações contábeis e financeiras	6(1)(c) Obrigação legal (Lei das Finanças de 1998, Lei das Sociedades de 2006)	n / D	Faturas, folha de pagamento, recibos, relatórios orçamentários	6 anos a partir do final do ano fiscal (conforme orientação do HMRC)
15	Contratos de apólices de seguro	6(1)(c) Obrigação legal	n / D	Documentos de apólice, termos de cobertura	6 anos a partir do vencimento da apólice
16	Apólices de seguro de responsabilidade civil da empregadora	6(1)(c) Obrigação legal	n / D	Nome da segurada, detalhes da cobertura, números de certificados	40 anos a partir do vencimento da apólice
17	Documentação de apoio para projetos financiados pela UE	6(1)(c) Obrigação legal (condições de subvenção UE/Reino Unido)	n / D	Planos de projeto, registros de trabalhadoras, orçamentos, registros de participantes	cinco anos após o último pagamento/recuperação da UE para o projeto.

Para obter mais informações sobre por quanto tempo armazenamos suas informações pessoais ou os critérios que usamos para determinar isso, entre em contato conosco usando os detalhes fornecidos acima.

Com quem compartilhamos informações

Processadores de dados

Lamplight - Sistema CRM: Este processador de dados realiza as seguintes atividades para nós: gerenciamento de dados das usuárias de serviços .

Outros com quem compartilhamos informações pessoais

- Organizações de caridade e voluntárias
- Prestadores de cuidados
- Organizações com as quais precisamos compartilhar informações por motivos de proteção
- Serviços de emergência em caso de perigo iminente ou risco de vida de alguém
- Órgãos ou autoridades legais
- Autoridades ou conselhos locais
- Autoridades reguladoras relevantes
- Organizações com as quais somos legalmente obrigados a compartilhar informações pessoais
- Consultores profissionais

Como reclamar

Caso tenha alguma preocupação sobre o uso que fazemos dos seus dados pessoais, você pode nos fazer uma reclamação usando os detalhes de contato no topo deste aviso de privacidade.

Se você continuar insatisfeita com a forma como usamos seus dados depois de registrar uma reclamação conosco, você também pode reclamar com o ICO.

Endereço do ICO:

Gabinete do Comissário de Informação

Casa Wycliffe

Travessa das Águas

Wilmslow

Cheshire

SK9 5AF

Número da linha de apoio: 0303 123 1113

Site: <https://www.ico.org.uk/make-a-complaint>

Última atualização em julho de 2025

Apêndice 6: AVISO DE PRIVACIDADE DE LAWRS PARA FUNCIONÁRIAS E VOLUNTÁRIAS

Aviso de privacidade para funcionárias /voluntárias do Serviço pelos Direitos da Mulher Latino-americana

Este aviso de privacidade informa o que você pode esperar que façamos com suas informações pessoais quando você trabalha conosco.

- Detalhes de contato
- Quais informações coletamos, usamos e por quê
- Bases legais e direitos de proteção de dados
- De onde obtemos informações pessoais
- Por quanto tempo mantemos as informações
- Com quem compartilhamos informações
- Como reclamar

Detalhes de contato

Correio: Serviço pelos Direitos da Mulher Latino-americana, 52-54 Featherstone Street, LONDRES, EC1Y 8RT, GB

Telefone: 0808 145 4909

E-mail: lawrs@lawrs.org.uk

Quais informações coletamos e usamos e por quê

Recrutamento, administração e gestão de pessoal

Coletamos ou usamos as seguintes informações pessoais como parte do recrutamento, administração e gerenciamento de pessoal:

- Dados de contato (por exemplo, nome, endereço, número de telefone ou endereço de e-mail pessoal)
- Data de nascimento
- Número do Seguro Nacional
- Gênero
- Cópias de passaportes ou outros documentos de identificação com foto
- Detalhes do parente mais próximo ou contato de emergência
- Histórico de emprego (por exemplo, candidatura a emprego, referências de emprego ou emprego secundário)
- Informações sobre o direito ao trabalho
- Detalhes de quaisquer condenações criminais (por exemplo, verificações do DBS)

Também coletamos ou utilizamos as seguintes informações de categorias especiais para recrutamento, administração e gestão de pessoal. Essas informações estão sujeitas a proteção adicional devido à sua natureza sensível:

- Origem racial ou étnica

Salários e pensões

Coletamos ou usamos as seguintes informações pessoais como parte do gerenciamento de salários e pensões:

- Cargo e contrato de trabalho (por exemplo, datas de início e saída, salário, alterações no contrato de trabalho ou padrões de trabalho)
- Tempo gasto trabalhando (por exemplo, planilhas de ponto ou registro de entrada e saída)
- Despesas, horas extras ou outros pagamentos demandados
- Licença (por exemplo, licença médica, férias ou licença especial)
- Licença-maternidade, paternidade, parentalidade compartilhada e licença de adoção e remuneração
- Detalhes da pensão
- Detalhes da conta bancária

Bases legais e direitos de proteção de dados

De acordo com a lei de proteção de dados do Reino Unido, precisamos ter uma "base legal" para coletar e usar suas informações pessoais. Há uma lista de possíveis bases legais no GDPR do Reino Unido. Você pode descobrir mais sobre bases legais no site do ICO.

A base legal que utilizamos pode afetar seus direitos de proteção de dados, que são resumidamente descritos abaixo. Você pode se informar mais sobre seus direitos de proteção de dados e as isenções que podem ser aplicadas no site do ICO:

- Seu direito de acesso - Você tem o direito de nos solicitar cópias de suas informações pessoais. Você pode solicitar outras informações, como detalhes sobre onde obtemos informações pessoais e com quem as compartilhamos. Existem algumas exceções, o que significa que você pode não receber todas as informações solicitadas. Você pode ler mais sobre isso aqui.
- Seu direito de retificação - Você tem o direito de nos solicitar a correção ou exclusão de informações pessoais que considere imprecisas ou incompletas. Saiba mais sobre isso aqui.
- Seu direito de esquecimento/apagamento - Você tem o direito de nos solicitar a exclusão de suas informações pessoais. Saiba mais sobre isso aqui.
- Seu direito à restrição do processamento - Você tem o direito de nos solicitar a limitação do uso de suas informações pessoais. Saiba mais sobre isso aqui.
- Seu direito de se opor ao processamento - Você tem o direito de se opor ao processamento dos seus dados pessoais. Saiba mais sobre isso aqui.
- Seu direito à portabilidade de dados - Você tem o direito de solicitar que transfiramos as informações pessoais que você nos forneceu para outra organização ou para você. Você pode ler mais sobre isso aqui.
- Seu direito de revogar o consentimento – Quando usamos o consentimento como base legal, você tem o direito de revogar seu consentimento a qualquer momento. Você pode ler mais sobre esse direito aqui.

Se você fizer uma solicitação, devemos responder sem demora injustificada e, em qualquer caso, dentro de um mês.

Para fazer uma solicitação de direitos de proteção de dados, entre em contato conosco usando os detalhes de contato no topo deste aviso de privacidade.

Nossas bases legais para a coleta e uso de seus dados

Nossas bases legais para coletar ou usar informações pessoais como parte do recrutamento, administração e gestão de pessoal são:

- Consentimento - obtivemos sua permissão após fornecermos todas as informações relevantes. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção. Para esclarecer, você tem o direito de revogar seu consentimento a qualquer momento.
- Contrato – precisamos coletar ou usar as informações para podermos celebrar ou executar um contrato com você. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção.
- Obrigação legal – precisamos coletar ou usar suas informações para cumprir a lei. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de apagamento, o direito de objeção e o direito à portabilidade de dados.
- Interesses legítimos – coletamos ou usamos suas informações para beneficiar você, nossa organização ou outra pessoa, sem causar risco indevido de danos a ninguém. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito à portabilidade. Nossos interesses legítimos são:
 - coletamos informações raciais ou étnicas e de gênero porque o recrutamento de LAWRS está aberto apenas para mulheres latino-americanas, de acordo com a Lei da Igualdade de 2010

Para obter mais informações sobre nosso uso de interesses legítimos como base legal, entre em contato conosco usando os detalhes de contato definidos acima.

Nossas bases legais para coletar ou usar informações pessoais como parte do gerenciamento de salários e pensões são:

- Contrato – precisamos coletar ou usar as informações para podermos celebrar ou executar um contrato com você. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de objeção.
- Obrigação legal – precisamos coletar ou usar suas informações para cumprir a lei. Todos os seus direitos de proteção de dados podem ser aplicáveis, exceto o direito de apagamento, o direito de objeção e o direito à portabilidade de dados.

De onde obtemos informações pessoais

Coletamos suas informações nos seguintes lugares:

- Diretamente de você
- Pessoas fornecendo referências (externos ou internos)
- Administradores de pensões ou departamentos governamentais (por exemplo, HMRC e DWP)

Por quanto tempo mantemos as informações

	ATIVIDADE DE PROCESSAMENTO	Artigo 6º Base legal	Condição de categoria especial do art. 9	Dados típicos mantidos	Período de gatilho de retenção

1	Aconselhamento , defesa e documentação de caso	6(1)(b) Contrato (serviço solicitado pela usuária)	9(2)(d) Sem fins lucrativos com salvaguardas	Detalhes de contato, status imigratório , saúde, detalhes dos filhos , encaminhamentos, notas de caso	6 anos após o último registro de caso (os detalhes do contrato da creche armazenados no Google Drive serão excluídos 1 ano após o último acesso ao serviço da creche)
2	Referências ou divulgações de proteção (não registradas no Lamplight, conforme especificado nas políticas de proteção do LAWRS)	6(1)(d) Interesses vitais	9(2)(c) Interesses vitais	Como acima + notas de risco	Até a conclusão da investigação legal + 1 ano
3	Recrutamento	6(1)(f) Interesses legítimos	Base do artigo 10 da DPA 2018, Anexo 1, Parte 1, parágrafo 1 – Emprego e proteção	CV, detalhes de contato, notas de entrevista, formulários de candidatura	6 meses após o término do recrutamento
4	Monitoramento de igualdade de oportunidades e impacto (funcionárias e voluntárias candidatas a emprego)	6(1)(f) Interesses legítimos	9(2)(g) Interesse público substancial – igualdade	Etnia, orientação sexual, deficiência	Anonimizar após o relatório anual e, em seguida, excluir os dados brutos
5	Atualizações por e-mail, SMS e correio sobre os serviços de LAWRS	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, e-mail, preferência de idioma	Até que o consentimento seja retirado ou 2 anos de inatividade

6	Gestão de RH e Voluntariado	6(1)(b) Contrato	9(2)(b) Direito do emprego e da segurança social	Referências , verificações DBS, informações de saúde, formulários de candidatura para voluntárias (formulário do Google)	6 anos para trabalhadoras e 2 anos para voluntárias - após o término do emprego/voluntariado
7	Registros do conselho e de governança	6(1)(c) Obrigação legal (Lei das Sociedades, Lei das Instituições de Caridade)	n / D	Detalhes de contato das membras do conselho gestor, , atas	Ata da diretoria – permanente; dados pessoais – 6 anos após o mandato
8	Registros de incidentes de saúde e segurança	6(1)(c) Obrigação legal	9(2)(f) Demandas legais	Relatórios de lesões, declarações de testemunhas	40 anos a partir do incidente (regulamentos de responsabilidade da empregadora)
9	Respostas do formulário do Google para eventos	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, endereço de e-mail, número de telefone, data de nascimento, idioma	Incluir dados anonimizados no Lamplight e excluir dados após o evento
10	Formulário do Google (encaminhamentos)	6(1)(a) Consentimento	n/a (sem dados de categoria especial)	Nome, endereço de e-mail, número de telefone, data de nascimento, idioma,	Carregar resposta no Lamplight e eliminar resposta
11	Registros de Reclamações	6(1)(f) Interesses legítimos	N/A (a menos que a reclamação inclua dados de categoria	Nome do reclamante, detalhes de contato, detalhes do	3 anos após a resolução da reclamação

			especial – então 9(2)(f) Demandas legais)	incidente, notas do caso, resultados	
12	Pesquisa e coleta de evidências	6(1)(f) Interesses legítimos	9(2)(j) Fins de pesquisa com salvaguardas (se forem utilizados dados pessoais)	Respostas de pesquisas, dados anônimos de usuáries de serviços, informações demográficas	5 anos após a publicação
13	Informações sobre fornecedores, prestadores e contratados	6(1)(b) Contrato	n / D	Nome, detalhes de contato comercial, termos do contrato, registros de pagamento	6 anos após o término do contrato (conforme Lei de Prescrição de 1980)
14	Informações contábeis e financeiras	6(1)(c) Obrigação legal (Lei das Finanças de 1998, Lei das Sociedades de 2006)	n / D	Faturas, folha de pagamento, recibos, relatórios orçamentários	6 anos a partir do final do ano fiscal (conforme orientação do HMRC)
15	Contratos de apólices de seguro	6(1)(c) Obrigação legal	n / D	Documentos de apólice, termos de cobertura	6 anos a partir do vencimento da apólice
16	Apólices de seguro de responsabilidade e civil da empregadora	6(1)(c) Obrigação legal	n / D	Nome da segurada, detalhes da cobertura, números de certificados	40 anos a partir do vencimento da apólice

17	Documentação de apoio para projetos financiados pela UE	6(1)(c) Obrigação legal (condições de subvenção UE/Reino Unido)	n / D	Planos de projeto, registros de trabalhador as, orçamentos, registros de participante s	cinco anos após o último pagamento/recuperação da UE para o projeto.
----	---	---	-------	---	--

Para obter mais informações sobre por quanto tempo armazenamos suas informações pessoais ou os critérios que usamos para determinar isso, entre em contato conosco usando os detalhes fornecidos acima.

Com quem compartilhamos informações

Em algumas circunstâncias, podemos compartilhar informações com as seguintes organizações:

- Fornecedores de treinamento
- HMRC
- Planos de benefícios para trabalhadoras
- Fornecedores de saúde e benefícios
- Auditores externos
- Fornecedores e prestadores de serviços
- Consultores profissionais

Processadores de dados

Utilizamos os seguintes processadores de dados pelos seguintes motivos:

Lamplight

Este processador de dados realiza as seguintes atividades para nós: adicionar e remover operadores de banco de dados, gerenciar usuárias de serviços de banco de dados.

Bright HR

Este processador de dados realiza as seguintes atividades para nós: treinamento de funcionárias e voluntárias, cursos on-line.

Como reclamar

Caso tenha alguma preocupação sobre o uso que fazemos dos seus dados pessoais, você pode nos fazer uma reclamação usando os detalhes de contato no topo deste aviso de privacidade.

Se você continuar insatisfeita com a forma como usamos seus dados depois de registrar uma reclamação conosco, você também pode reclamar com o ICO.

Endereço do ICO:

Gabinete do Comissário de Informação

Casa Wycliffe

Travessa das Águas

Wilmslow

Cheshire

SK9 5AF

Número da linha de apoio: 0303 123 1113

Site: <https://www.ico.org.uk/make-a-complaint>

Última atualização em julho de 2025

Apêndice 7: Avaliação de Impacto sobre a Proteção de Dados (AIPD)

Informações do Projeto/Serviço

Título do projeto/serviço/atividade	
Líder do Projeto	
Financiador (se aplicável)	
Dados pessoais serão processados?	☐ Sim ☐ Não (se não, o DPIA termina aqui)

Resumo da atividade

Descreva brevemente a finalidade do projeto ou serviço, porque dados pessoais são necessários e o que será feito com eles.

Requisitos de dados

De quem os dados serão processados? ☐ Usuárias ☐ Trabalhadoras ☐ Voluntárias ☐ Crianças ☐ Público
Número aproximado de pessoas: ☐ 1–50 ☐ 50–100 ☐ 100–300 ☐ 300+
Quais dados pessoais serão usados? (por exemplo, nome, e-mail, número de telefone etc.)

Dados sensíveis (categoria especial) ou de condenação criminal? ☐ Sim ☐ Não Em caso afirmativo, especifique:			
Base legal para processamento			
Dados pessoais (não sensíveis)		Sensível (dados de categoria especial)	
Consentimento	☐	Consentimento explícito	☐
Contrato	☐	Emprego (direito social)	☐
Obrigação legal	☐	Interesses vitais (salv guarda)	☐
Interesses vitais (salv guarda)	☐	Dados criminais (DPA Anexo 1: LAWRS é exigido por lei)	☐
Uso de Dados			
Onde os dados serão armazenados? ☐ Google Drive ☐ Lamplight Quem terá acesso? (Liste as funções, não os nomes): Os dados serão compartilhados com alguém fora de LAWRS? ☐ Sim ☐ Não Se sim, quem e porquê: Será transferido para fora do Reino Unido? ☐ Sim ☐ Não Se sim, como serão protegidos?			
Segurança e retenção Como os dados serão protegidos? (por exemplo, criptografia, senhas acesso baseadas em funções): Período de retenção: Como os dados serão excluídos com segurança após o uso?			
Transparência e direitos O Aviso de Privacidade foi compartilhado com os titulares dos dados? ☐ Sim ☐ Não As pessoas podem retirar o consentimento ou optar por não participar? ☐ Sim ☐ Não			

Avaliação de risco

O que poderia dar errado (por exemplo, vazamento de dados, acesso não autorizado)?

Que medidas serão tomadas para reduzir o risco?

Revisão e aprovação

Concluído por (líder do projeto): _____

DPO revisado: _____

Data de conclusão: _____

Próxima revisão prevista para: _____ (geralmente 1 ano)