

Política de privacidade global

Documento	Política de privacidade global
Objetivo	Regulamentar objetivos e critérios para o tratamento de dados pessoais.
Aprovador	Comité de Risco e Conformidade (" CRC ")

Confidencialidade - A distribuição deste documento é limitada a todas as entidades do Grupo Uriach e aos seus parceiros comerciais. Não deve ser distribuído sem o consentimento do Conselho de Administração.

00 TERMOS

Os termos utilizados na presente Política Global de Privacidade (a "**Política**") terão o significado definido no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE ("**RGPD**"), exceto se outro significado for expressamente definido na presente Política

01 OBJETIVO

O objetivo desta Política é garantir que cada empresa da Uriach cumpre os regulamentos de proteção de dados aplicáveis, ou seja, o RGPD e os regulamentos locais de cada território em que a Uriach opera (os "**Regulamentos de PD aplicáveis**").

Esta Política será adaptada às alterações legislativas nos países em que a Uriach opera, bem como aos critérios definidos pela autoridade de controlo local competente, pelo Comité Europeu para a Proteção de Dados ("**ECDC**") e pelas decisões dos tribunais competentes.

02 ÂMBITO DE APLICAÇÃO

O âmbito de aplicação da presente política inclui o seguinte:

- a) **Âmbito Corporativo** - A presente Política aplica-se a todas as empresas pertencentes à Uriach, bem como às empresas subsidiárias e participadas sobre as quais a Uriach exerce um controlo efetivo ou detém cargos nos órgãos de gestão.
- b) **Pessoal** - A presente política aplica-se a todos os níveis da organização, incluindo a direção, os quadros superiores, os órgãos de supervisão e todo o pessoal.
- c) **Âmbito relacional** - O âmbito de aplicação da presente Política estender-se-á, na medida do possível, a fornecedores, clientes, empresas subcontratadas ou colaboradores.
- d) **Âmbito geográfico** - Esta Política aplica-se a qualquer área geográfica onde a Uriach tenha as suas instalações, quer seja local ou internacional.

Quaisquer exceções às regras estabelecidas na presente Política estão sujeitas à aprovação explícita do Comité de Risco e Conformidade ("**CRC**"). Em caso de discrepância ou dúvida relativamente à presente política, o departamento jurídico fornecerá orientações e assistência relevantes.

03 ATIVIDADES E RISCOS DO TRATAMENTO DE DADOS PESSOAIS

A principal atividade da Uriach é o setor da saúde. As operações de tratamento de dados pessoais mais comuns neste setor são as seguintes:

1. Recrutamento de pessoal
2. Gestão do emprego
3. Relações dos clientes B2C
4. Relações com clientes B2B
5. Relações com os fornecedores
6. Marketing
7. Atendimento ao cliente
8. Farmacovigilância, cosmetovigilância
9. Ensaio clínicos, estudos observacionais
10. Comércio eletrónico
11. Financeiro

12. Jurídico

Os principais riscos decorrentes do não cumprimento das obrigações legais previstas nos Regulamentos aplicáveis às PD são os seguintes

13. Sanções administrativas
14. Intervenção regulamentar
15. Problemas de qualidade
16. Danos
17. Danos à reputação
18. Infrações à privacidade

A proteção de dados pessoais é um objetivo prioritário para a Uriach e requer uma série de medidas legais, técnicas e organizacionais que se encontram resumidas nesta Política e que serão definidas nas regras, protocolos e/ou procedimentos relevantes da empresa.

04 PRINCÍPIOS DA PROTEÇÃO DE DADOS

- a) **Legalidade:** Apenas serão tratados os dados pessoais para os quais a Uriach tem uma base legítima estabelecida por lei.
- b) **Transparência:** A Uriach informará os titulares dos dados, de forma clara e simples, de todas as circunstâncias relacionadas com o tratamento.
- c) **Equidade:** A Uriach não tratará os dados pessoais em circunstâncias diferentes das referidas.
- d) **Limitação da finalidade:** A Uriach recolherá os dados pessoais para fins específicos, explícitos e legítimos e não os processará de forma incompatível com esses fins.
- e) **Minimização dos dados:** Os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados.
- f) **Exatidão:** Os dados pessoais devem ser exatos e, se necessário, atualizados, e a Uriach tomará todas as medidas razoáveis para assegurar que os dados pessoais inexatos em relação às finalidades para que são tratados sejam apagados ou retificados sem demora.
- g) **Limitação da conservação:** A Uriach conservará os dados pessoais de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para que foram recolhidos.
- h) **Integridade e confidencialidade:** A Uriach tratará os dados pessoais de forma a garantir a segurança adequada, através da aplicação de medidas técnicas e organizativas apropriadas. Os dados pessoais só serão acessíveis às pessoas autorizadas a aceder aos mesmos e não podem ser comunicados a terceiros sem a correspondente autorização e base legal.
- i) **Responsabilidade:** Cada empresa da Uriach é responsável pelo cumprimento das disposições dos respetivos Regulamentos de PD aplicáveis e deve ser capaz de demonstrar esse cumprimento.

- j) **Proteção de dados desde a conceção e por defeito:** Na fase de conceção de novos tratamentos, projetos, serviços e produtos que impliquem o tratamento de dados pessoais, a Uriach procede a uma avaliação prévia do impacto sobre a proteção de dados.

05 ORGANISMOS DE CONTROLO, FUNÇÕES E RESPONSABILIDADES

Todos os funcionários da Uriach, independentemente do seu cargo, devem ser obrigados a cumprir as regras, procedimentos e controlos estabelecidos para cumprir os Regulamentos de PD aplicáveis.

O modelo de governação para garantir o bom desempenho da Uriach em matéria de proteção de dados é o seguinte:

- a) **Comité Mundial para a Proteção de Dados:** O Comité Global para a Proteção de Dados é responsável por tornar a presente política eficaz através da aplicação das diferentes medidas previstas.

O Comité Global para a Proteção de Dados será composto, como membros permanentes, pelas pessoas da Uriach que, em qualquer momento, ocupem o cargo de:

- Diretor Jurídico e de Sustentabilidade - Presidente
- Diretor Jurídico e de Conformidade e nomeado DPO na sede - Secretário
- Diretor Global de Dados e Tecnologia - Membro
- Especialista em Cibersegurança - Membro
- Diretor Global Digital e de Dados - Membro

Espera-se que os membros do Comité Global para a Proteção de Dados mantenham um conhecimento atualizado dos requisitos legais e regulamentares relevantes, promovam regulamentos adicionais que implementem esta Política, bem como proporcionem formação a todos os funcionários.

- b) **Responsáveis locais pela proteção de dados:** Dependendo das necessidades locais e da legislação aplicável, os responsáveis locais pela proteção de dados (DPO) podem ser nomeados e oficialmente designados para as autoridades de supervisão relevantes. Estes DPOs locais devem reportar ao Comité Global para a Proteção de Dados e são responsáveis por garantir a conformidade com os regulamentos de proteção de dados nos respetivos territórios.
- c) **Membros da Organização:** Todos os membros da organização são responsáveis pelo cumprimento dos regulamentos de proteção de dados aplicáveis e pelo desenvolvimento correto da Política.

Todos os membros da Organização, independentemente do cargo que ocupem, podem

- assegurar o cumprimento das disposições da presente política,
- responder imediatamente a quaisquer indicações que possam receber do Comité Mundial para a Proteção de Dados, e
- consultar o Comité Global para a Proteção de Dados se tiver alguma dúvida sobre a interpretação desta Política ou sobre a aplicação dos Regulamentos de PD aplicáveis.

Do mesmo modo, todos os membros da Organização devem notificar imediatamente o Comité Mundial para a Proteção de Dados de qualquer ação destinada a prevenir ou remediar a eventual prática de infrações à presente política.

06 REGISTO DAS ATIVIDADES DE TRATAMENTO

Cada empresa da Uriach implementará um Registo de Atividades de Tratamento ("**RAT**"). As operações de tratamento incluídas neste RAT são o resultado de uma análise efetuada através de entrevistas com todos os departamentos que possam tratar dados pessoais no exercício das suas funções.

O RAT deve ser atualizado regularmente para fornecer uma imagem atualizada do tratamento efetuado por cada empresa da Uriach.

07 DIREITOS DAS PESSOAS EM CAUSA

Cada empresa da Uriach facilitará o exercício dos direitos dos titulares dos dados, quer atuando como responsável pelo tratamento, quer como subcontratante. Além disso, deve implementar regras, procedimentos ou protocolos adequados em relação ao acima exposto.

08 CONTROLO DOS FORNECEDORES

O processo de aprovação dos fornecedores da Uriach incluirá um controlo preliminar para confirmar, nomeadamente, se o fornecedor em causa exigirá o tratamento de dados pessoais para fornecer os seus serviços ou bens.

Para tal, o controlo prévio permitirá selecionar os fornecedores e realizar um processo de avaliação e aprovação prévia.

Cada empresa da Uriach pode elaborar regras e procedimentos para desenvolver, especificar e pormenorizar o conteúdo da presente secção. Em particular, mas não limitado a, cada empresa da Uriach utilizará apenas subcontratantes que ofereçam garantias suficientes de aplicação de medidas técnicas e organizativas adequadas, de modo a que o tratamento cumpra os requisitos dos Regulamentos de PD aplicáveis e assegure a proteção dos direitos dos titulares dos dados.

09 TRANSFERÊNCIAS INTERNACIONAIS

A Uriach só transferirá dados pessoais para um país terceiro ou uma organização internacional fora do Espaço Económico Europeu ("**EEE**") com base no seguinte:

1. uma decisão de adequação;
2. salvaguardas adequadas, como as cláusulas contratuais-tipo ("**CCP**");
3. regras vinculativas para as empresas
4. uma autorização da autoridade de controlo competente; ou
5. derrogações para situações específicas.

10 PERÍODOS DE RETENÇÃO DE DADOS

As empresas da Uriach conservam os dados pessoais de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para as finalidades para as quais os dados são tratados.

As empresas devem elaborar e atualizar um regime que estabeleça o período de conservação dos dados que devem ou consideram adequado conservar, de acordo com os respetivos

regulamentos aplicáveis em matéria de proteção de dados. Este regime deve ter em conta o prazo de prescrição das infrações e as limitações estabelecidas nos Regulamentos de PD aplicáveis, bem como as obrigações legais, setoriais e contratuais que possam exigir períodos de conservação mais longos.

As empresas da Uriach devem informar os titulares dos dados sobre os períodos de retenção quando os seus dados são recolhidos.

11 AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS ("DPIA")

As empresas da Uriach devem avaliar a necessidade de realizar uma DPIA de acordo com os respetivos Regulamentos de PD aplicáveis e, se necessário, realizá-la antes do início da atividade de processamento de dados relevante.

12 RESPONSÁVEL PELA PROTEÇÃO DE DADOS ("DPO")

Cada empresa da Uriach deve efetuar uma avaliação da necessidade de nomear um DPO de acordo com os respetivos regulamentos de PD aplicáveis.

A necessidade de nomear um DPO deve ser imediatamente comunicada ao Comité Mundial para a Proteção de Dados (dpo@uriach.com)

13 MEDIDAS DE SEGURANÇA

Cada empresa da Uriach implementará medidas técnicas e organizacionais adequadas para garantir um nível de segurança apropriado aos riscos. Para o efeito, cada organização tem de considerar o estado da técnica, os custos de implementação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares.

14 VIOLAÇÃO DE DADOS E COMUNICAÇÃO DE RISCOS

A Uriach implementará protocolos para lidar com violações de dados e para garantir que são tomadas medidas adequadas, tanto preventivas como reativas, e para notificar, quando necessário, as autoridades de controlo competentes no prazo de 72 horas e/ou para comunicar a violação aos titulares dos dados afetados.

Qualquer violação de dados deve ser imediatamente comunicada ao Comité Mundial para a Proteção de Dados.

15 AUDITORIA DA PROTEÇÃO DE DADOS

A Uriach efetuará auditorias periódicas para avaliar os riscos referidos na presente Política e para assegurar o cumprimento dos respetivos Regulamentos de PD aplicáveis.

Esta auditoria pode ser interna, externa ou mista e deve incluir uma verificação da existência, adequação e eficácia das medidas e controlos em vigor para evitar violações das regras relativas à proteção dos dados pessoais.

O âmbito desta auditoria será diferente do da avaliação de impacto, na medida em que a avaliação de impacto diz respeito a uma operação de tratamento específica, enquanto a auditoria à proteção de dados diz respeito à conformidade de toda a organização com os regulamentos aplicáveis em matéria de proteção de dados.

16 FORMAÇÃO E SENSIBILIZAÇÃO

A Uriach promoverá a formação e a sensibilização constantes para a proteção de dados a todos os níveis da organização, a fim de melhorar a sensibilização da organização para a proteção dos dados pessoais.

O acima exposto deve ser realizado quer em sessões presenciais, quer em cursos de e-learning ou qualquer outro tipo de materiais e ferramentas de comunicação e formação para aumentar a sensibilização para os riscos de infração a todos os níveis da organização.

17 ATUALIZAÇÃO E APLICAÇÃO DA PRESENTE POLÍTICA

A presente política e a sua aplicação devem ser revistas regularmente. Qualquer alteração deve ser aprovada pelo CRC

*

*

*